2014-02-24 Games to establish structure in an unknown Hilbert space

Monday, February 24, 2014 9:30 AM

Outline:

Problem
CHSH game rigidity
Sequential CHSH games

GAMES TO ESTABLISH STRUCTURE IN AN UNKNOWN HILBERT SPACE

Ben Reichardt
USC

How can we characterize/control an experimental system or device?
* with very high confidence *

Obvious problem:

Systems are quantum mechanical

→ Exponentially complex to describe

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

→ Limited access: measurements give classical information

More subtle problem:

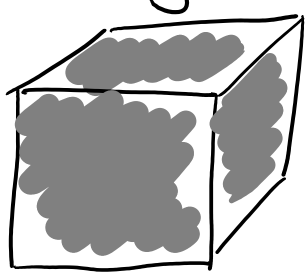
What can go wrong?

Example: To generate a random bit,

- Prepare $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Measure it

Obvious problems	Subtle problems	Now you're just paranoid
Bias in the random bit	Small correlations between successive runs	Device looks correct, but hidden inside is a preprogrammed random string

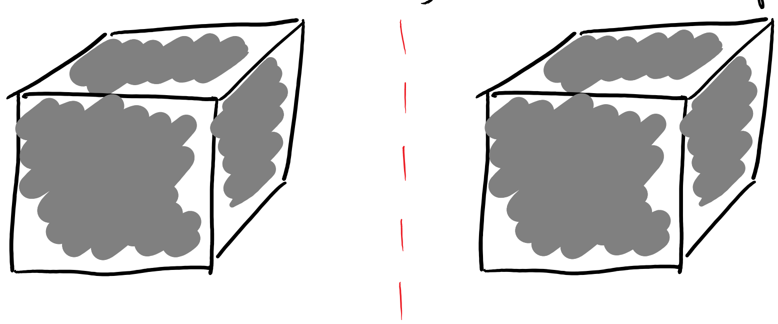
Our security model: (maximally conservative)



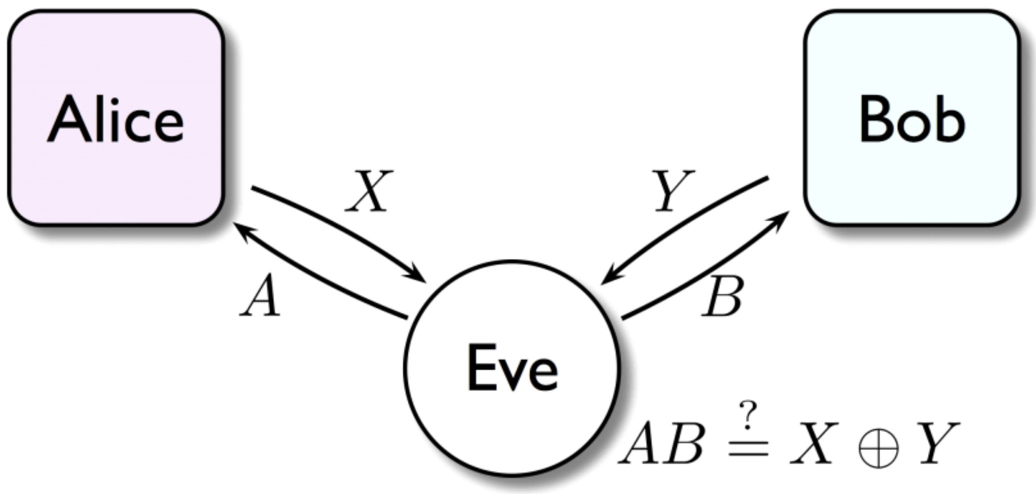
black-box device made by an adversary!

Of course, it's hopeless to guarantee, e.g., that the box outputs a fresh, uniformly random string.

But with **two devices**, that becomes possible.



CHSH game:

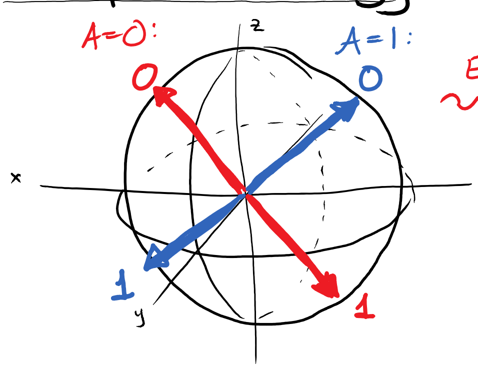


Best classical strategy:

Output $X = Y = 0$ (or 1)

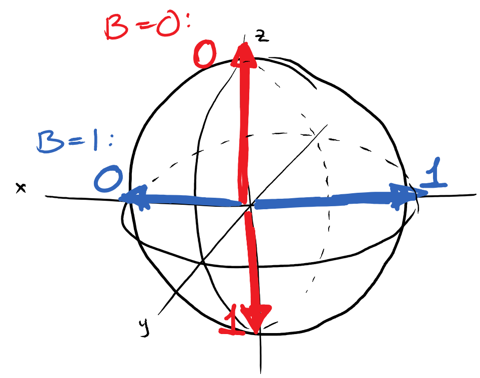
→ wins if $AB = 0$, 3/4 of the time

Best quantum strategy:



EPR pair

$|00\rangle + |11\rangle$



Observe: If both inputs are 0, or one is 0 & other 1,

$$\mathbb{P}[X = Y] = \cos^2 \frac{\pi}{8}.$$

If both inputs are 1,

$$\mathbb{P}[X \neq Y] = \cos^2 \frac{\pi}{8}.$$

⇒ wins $\cos^2 \frac{\pi}{8} \approx 85\%$ of the time

This gap — 75% for classical devices, 85% for quantum — has traditionally been used to test that systems are quantum-mechanical. But we'll go much further...

General quantum strategy:

Alice & Bob share arbitrary quantum state (density matrix)
in product of arbitrary Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$,
make arbitrary two-outcome projective measurements (depending on A,B).

Theorem: If $\mathbb{P}[\text{win}] \geq \cos^2\frac{\pi}{8} - \varepsilon$,
then up to local isometries on $\mathcal{H}_A, \mathcal{H}_B$,

- initial state $\approx_{\sqrt{\varepsilon}} (|00\rangle + |11\rangle) \otimes (\text{more})$
- $\left(\begin{matrix}\text{effect of Alice \& Bob's} \\ \text{measurements on this state}\end{matrix}\right) \approx_{\sqrt{\varepsilon}} \left(\begin{matrix}\text{ideal measurement} \\ \text{strategy}\end{matrix}\right)$

Proof:
Two-outcome projective measurement $\longleftrightarrow$ hyperplane

Two hyperplanes (for inputs 0 and 1)
$\Rightarrow$ Consider dihedral angles
(in 2D)
$\Rightarrow$ Suffices to analyze case $\dim \mathcal{H}_A = 2 = \dim \mathcal{H}_B \ldots$ $\square$

Problem: How do we know if $\mathbb{P}[\text{win}] \geq \underbrace{\cos^2\frac{\pi}{8}}_{= \omega^*} - \varepsilon$?
Answer: Statistics!

- Play 10^6 games in a row.
- They could get lucky and win them all, but that's unlikely.
  They could also cheat in a few (play classically), and it would be lost in the noise.
- But if
$$\mathbb{P}\left[\text{win} \geq (\omega^* - \varepsilon) \cdot 10^6 \text{ games}\right] \geq 1 - \varepsilon$$
$\Rightarrow$ at the start of a **random game**, most likely $\mathbb{P}[\text{win that game}] \geq \omega^* - \varepsilon'$
$\Rightarrow$ Theorem applies

Idea: Repeated CHSH games give a test for quantum devices.

But more complex applications require more qubits' worth of entanglement.

$\boxed{\text{Tests}}$

- If devices pass the tests (w.h.p.), then they must share lots of entanglement, which they measure in a very particular way

MAIN THEOREM:

$$\underbrace{\underbrace{\times\ \times\ \times\ \times}_{n \text{ games}} \quad \underbrace{\times\ \times\ \times\ \times}_{n \text{ games}} \quad \underbrace{\times\ \times\ \times\ \times}_{n \text{ games}} \quad \cdots \quad \underbrace{\times\ \times\ \times\ \times}_{n \text{ games}}}_{\substack{N \text{ blocks of } n \\ \text{sequential CHSH games}}}$$

- If: $\mathbb{P}[\text{win} \geq \omega^* - \varepsilon \text{ of games}] \geq 1 - \varepsilon$
- Then: At the beginning of a random block of n games,

  Alice & Bob's strategy for those games $\approx$ Ideal strategy on $(|00\rangle + |11\rangle)^{\otimes n}$

  pair j for game j

Note: This gives lots of entanglement, in a very nice form (EPR pairs in tensor product, measured one at a time), somewhat inefficiently: $N = \text{poly}(n)$,

final error $= \varepsilon^{1/c}$.

Formally: $\approx$ means with super-operators, trace distance

projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ $\longrightarrow$ super-operator

$$\mathcal{E}(\rho) = \Pi \rho \Pi \otimes |0\rangle\langle 0| + \overline{\Pi} \rho \overline{\Pi} \otimes |1\rangle\langle 1|$$

Ideal strategy $\hat{\mathcal{E}}_A = \frac{1}{2}|0\rangle\langle 0| \otimes \overbrace{\sum_{x=0}^{1} \Pi^x_{A=0}\, \rho\, \Pi^x_{A=0}}^{\text{quantum result}} \otimes \overbrace{|x\rangle\langle x|}^{\text{classical outcome}}$

$$+ \frac{1}{2}|1\rangle\langle 1| \otimes \sim\!\sim\!/\!\!\sim\!\sim$$

input coin A — projective measurement (depending on A) — output X

"Alice & Bob's strategy for those games $\approx$ Ideal strategy on $(|00\rangle + |11\rangle)^{\otimes n}$
pair j for game j"

means that up to local isometries $\mathcal{H}_A \hookrightarrow (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_A'$
$\mathcal{H}_B \hookrightarrow (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_B'$,

$$\Big\| \underbrace{\mathcal{E}^{AB}_{1,j}}_{\substack{\text{joint super-operator} \\ \text{for games 1 to } j}}(\rho) - \underbrace{\hat{\mathcal{E}}^{AB}_{1,j}\big(n \text{ EPR pairs } \otimes (\text{more})\big)}_{\text{ideal strategy}} \Big\|_{\underline{\underline{tr}}} \approx 0.$$

trace distance

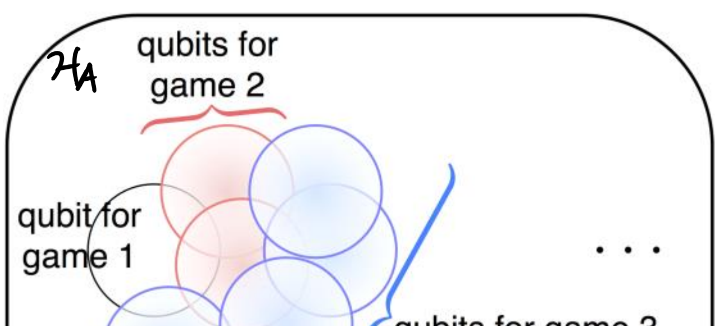
Proof sketch: 3 steps

⓪ Statistics:

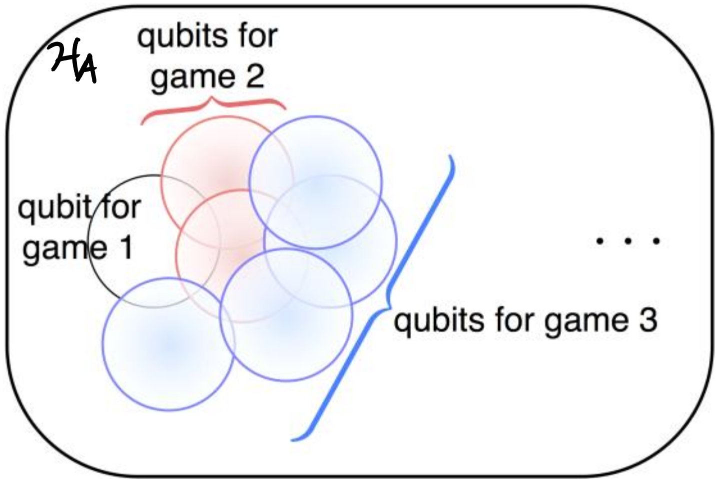
$\mathbb{P}[\text{win} \approx \omega^*$ of the games$] \approx 1$

$\Rightarrow$ In a random block of n games,
for every $j = 1, 2, \ldots, n$,
at the beginning of game j $\mathbb{P}[\text{win}] \approx \omega^*$
(for most outcomes of games 1 to $j-1$)

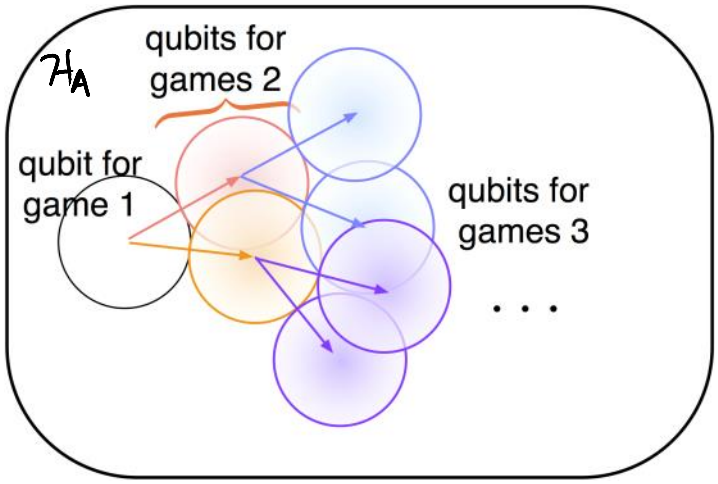
① Locate qubits used in every game (one-shot CHSH theorem)



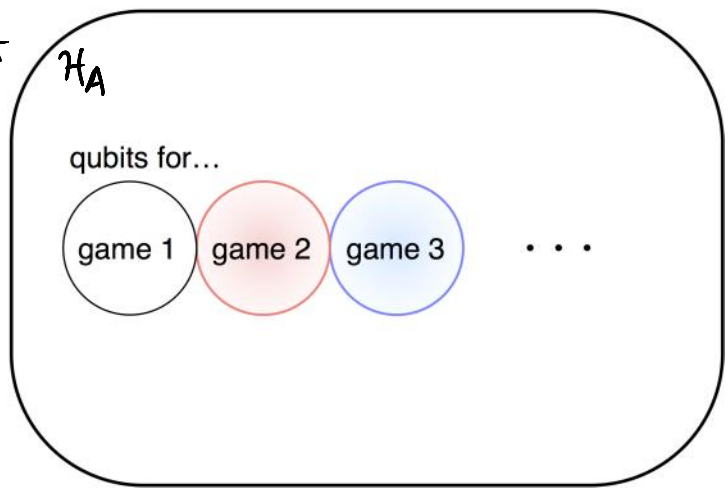
① Locate qubits used in every game (one-shot CHSH theorem)



② Qubits in sequential games are in tensor product

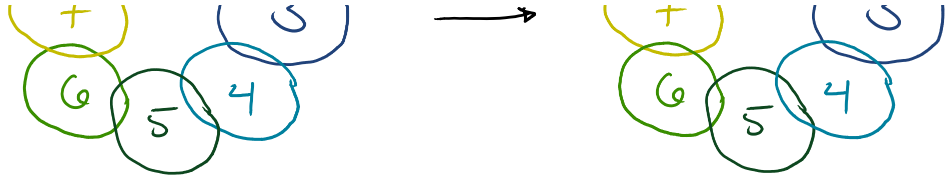


③ Qubit locations do not depend on history ✓



Step 2: Qubits in sequential games are in tensor product

What can go wrong?



slightly overlapping qubits in sequential games

accumulating errors allow for huge overlap later
— no tensor product structure

How do errors accumulate?

a) Small errors away from ideal could slowly move qubits

Example: 5 EPR pairs in tensor product

accumulated errors from games 1 to 4 move this qubit into position 1

— and errors can accumulate quickly!

$$|\psi\rangle \longmapsto \frac{\Pi|\psi\rangle}{\|\Pi|\psi\rangle\|} \quad + \sqrt{2}\cdot\text{error} \text{ if } \|\Pi|\psi\rangle\| = \tfrac{1}{\sqrt{2}}$$

+ error

b) Fixing earlier games breaks later games

Assume: $\mathbb{P}[\text{win game } 1] \geq \omega^* - \varepsilon$,
$\mathbb{P}[\text{win game } 2 \mid \text{game 1's outcome}] \geq \omega^* - \varepsilon$

Then: A & B's initial state & measurements are $\sqrt{\varepsilon}$-close to ideal,
At the beginning of game 2, measurements & current state are $\sqrt{\varepsilon}$-close to ideal.

Now fix game 1: Replace with ideal strategy

$\Rightarrow \mathbb{P}[\text{win game } 2 \mid \overset{\text{new}}{\text{game}}\ 1] \geq \omega^* - \varepsilon - \sqrt{\varepsilon}$

$\Rightarrow$ now strategy is $\varepsilon^{1/4}$-close to ideal ....

Instead, work backward:

Fixing game 2 does not affect game 1
— but you can only change the super-operators, not the underlying state

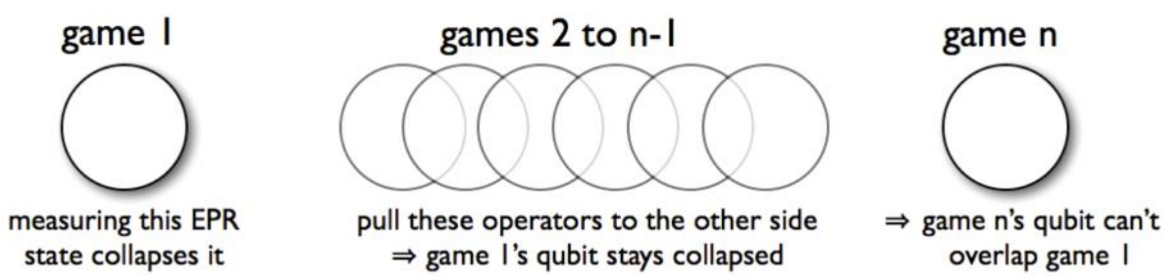
(if you fix the state at the beginning of game 2, that might not correspond to anything before game 1)
$\Rightarrow$ we fix super-operators going backward, and states going forward

Main idea: Leverage tensor-product structure *between* the boxes

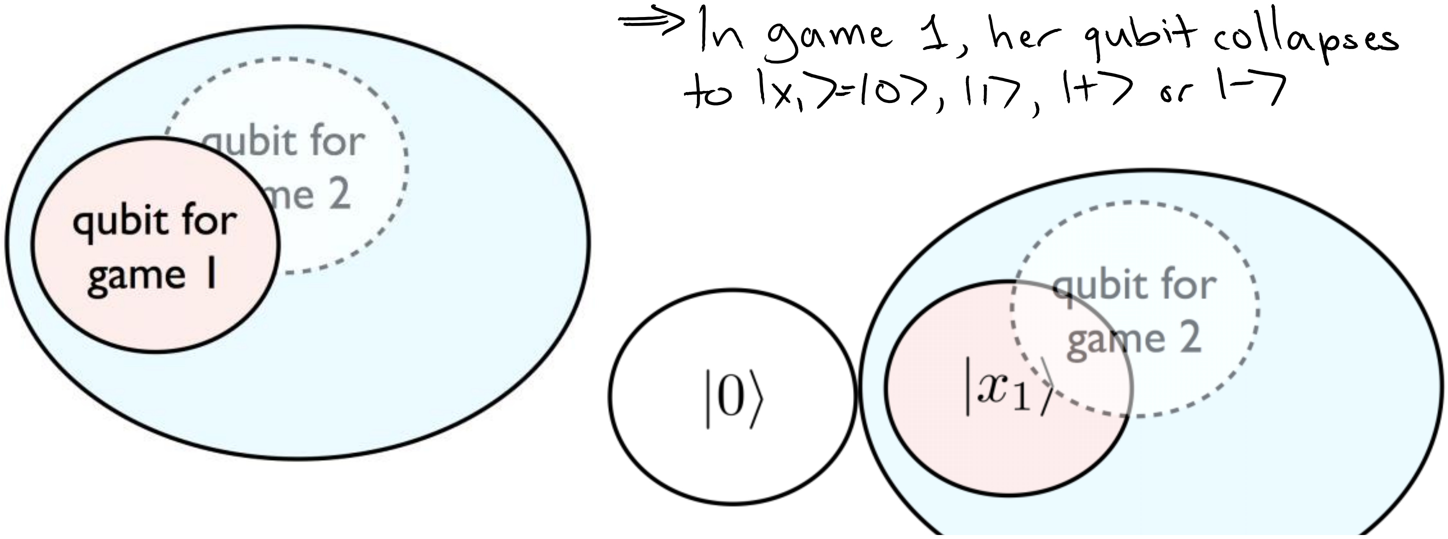
Fact 1: Operations on the first half of an EPR state can just as well be applied to the second half

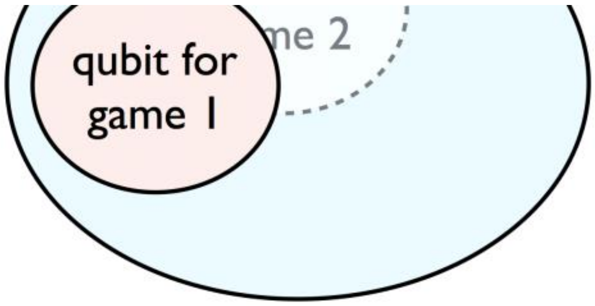
$$(M \otimes I)(|00\rangle + |11\rangle) = (I \otimes M^T)(|00\rangle + |11\rangle)$$

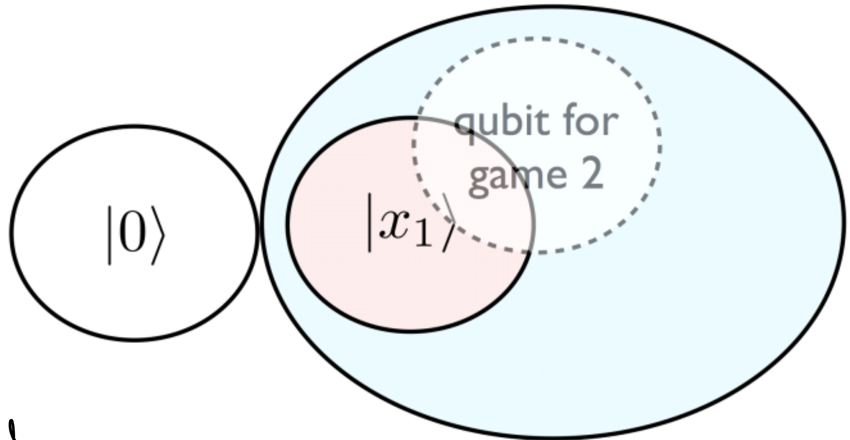
Fact 2: Quantum mechanics is local: An operation on the second half of a state can't affect the first half *in expectation*



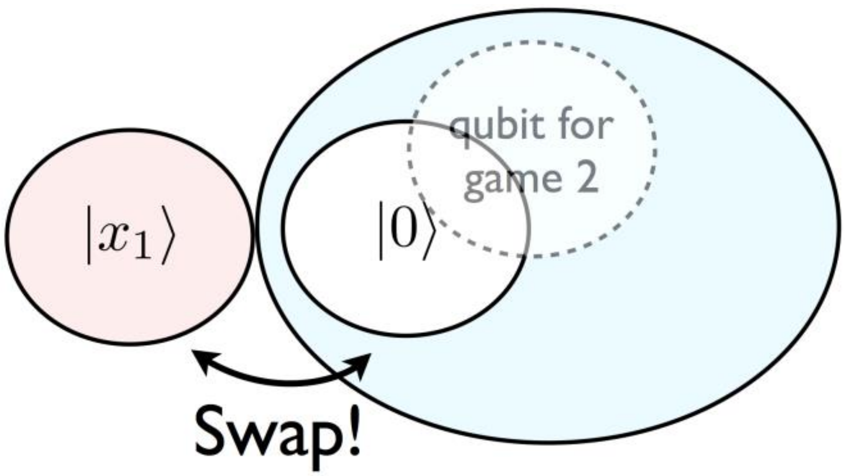
Formally:
Assume: Alice measures a qubit in every game, possibly overlapping
$\Rightarrow$ In game 1, her qubit collapses to $|x_1\rangle = |0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$



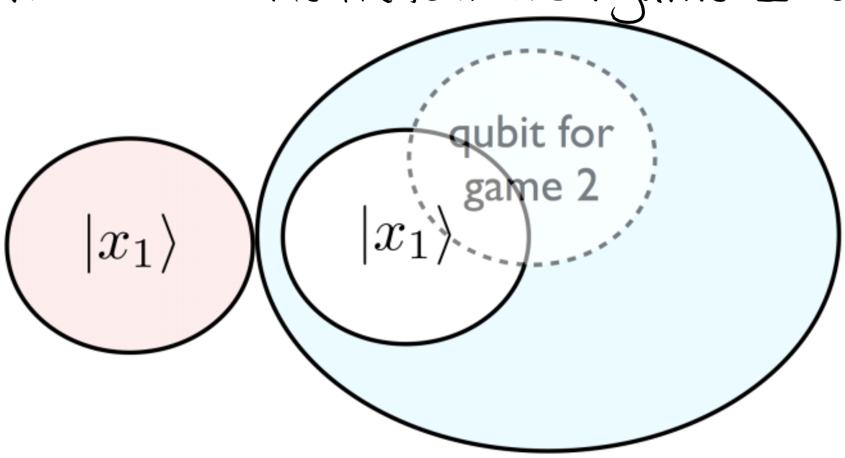




Add an ancilla $|0\rangle$ qubit, and swap it with game 1's qubit:



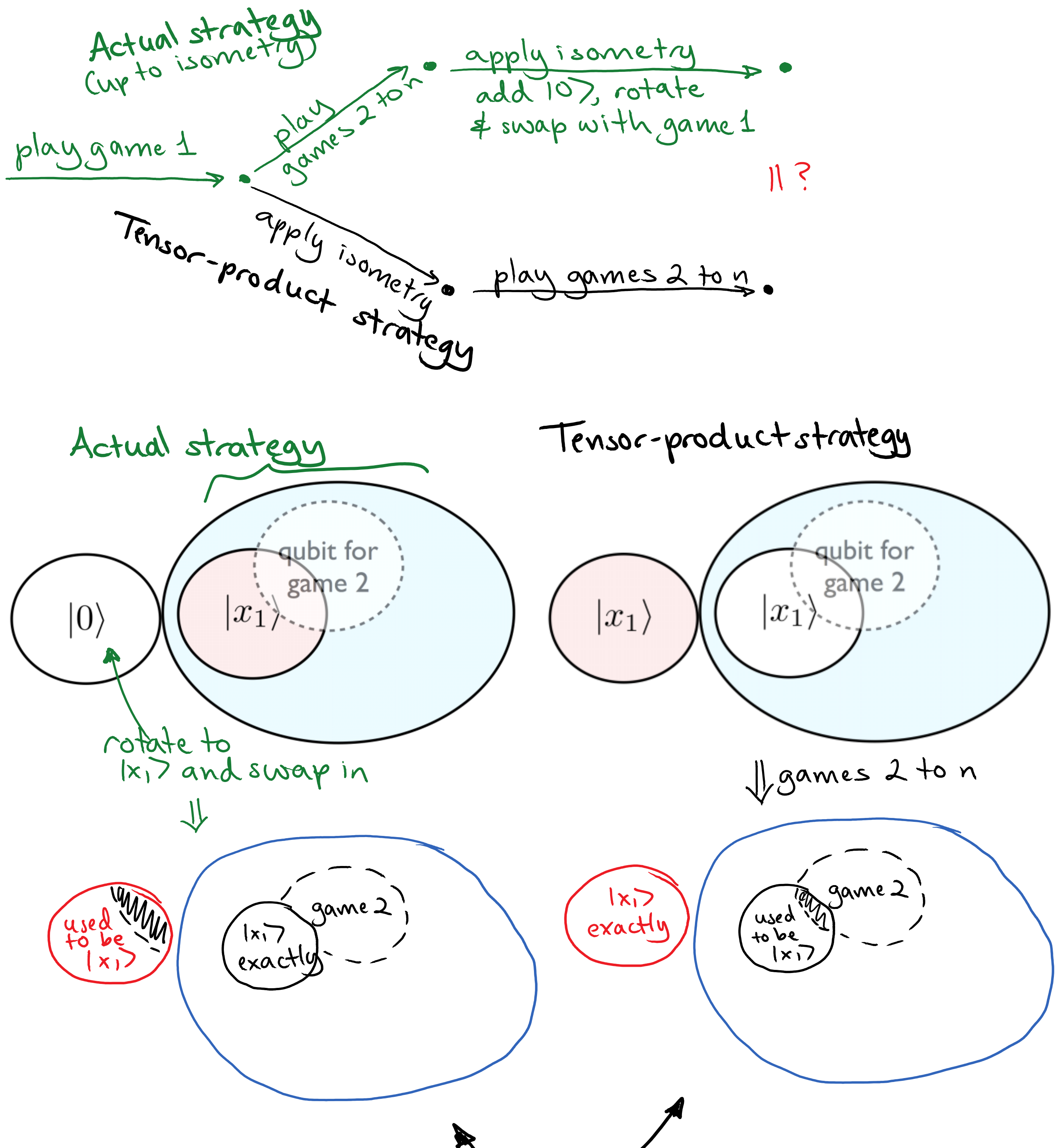
Rotate the ancilla to match game 1's outcome.



Now play remaining games here,
in a space in tensor product with game 1

This defines a tensor-product strategy (with history-dependent qubit locations).

Does it agree, up to isometry, with the **actual** strategy?



these are the same if $|x_1\rangle$ stays collapsed through games 2 to n.

Problem: Strategies ideal **together** versus **separately**

We know

$$\mathcal{E}^A_j(\rho_j) \approx \hat{\mathcal{E}}^A_j(\hat{\rho}_j)$$
$$\underbrace{\mathcal{E}^B_j(\rho_j)}_{\substack{\text{actual strategy} \\ \text{after finishing} \\ j-1 \text{ games}}} \approx \underbrace{\hat{\mathcal{E}}^B_j(\hat{\rho}_j)}_{\text{ideal strategy}}$$

$$\left[\rho_j = \mathcal{E}^{AB}_{1,j-1}(\rho_1)\right]$$

We **want** Alice & Bob's super-operators to be separately close to ideal

$$\mathcal{E}^A_{1,j}(\rho_1) \approx \hat{\mathcal{E}}^A_{1,j}(\hat{\rho}_1)$$
$$\underbrace{\mathcal{E}^B_{1,j}(\rho_1)}_{\text{actual separate strategies}} \approx \underbrace{\hat{\mathcal{E}}^B_{1,j}(\hat{\rho}_1)}_{\text{ideal separate strategies}}$$

Trick:

Given

$$\underbrace{\mathcal{E}^A_{1,j}\,\mathcal{E}^B_{1,j}(\rho_1)}_{\substack{\text{actual joint strategy} \\ \text{for } j \text{ games}}} \approx \underbrace{\hat{\mathcal{E}}^A_{1,j}\,\hat{\mathcal{E}}^B_{1,j}(\hat{\rho}_1)}_{\text{ideal joint strategy}}$$

Observe: After Bob's super-operator, EPR pairs are collapsed

$\Rightarrow$ Instead of measuring, Alice can just rotate her qubits unitarily

$$\hat{\mathcal{U}}^A_{1,j}\,\mathcal{E}^B_{1,j}(\rho_1) \approx \hat{\mathcal{U}}^A_{1,j}\,\hat{\mathcal{E}}^B_{1,j}(\hat{\rho}_1)$$

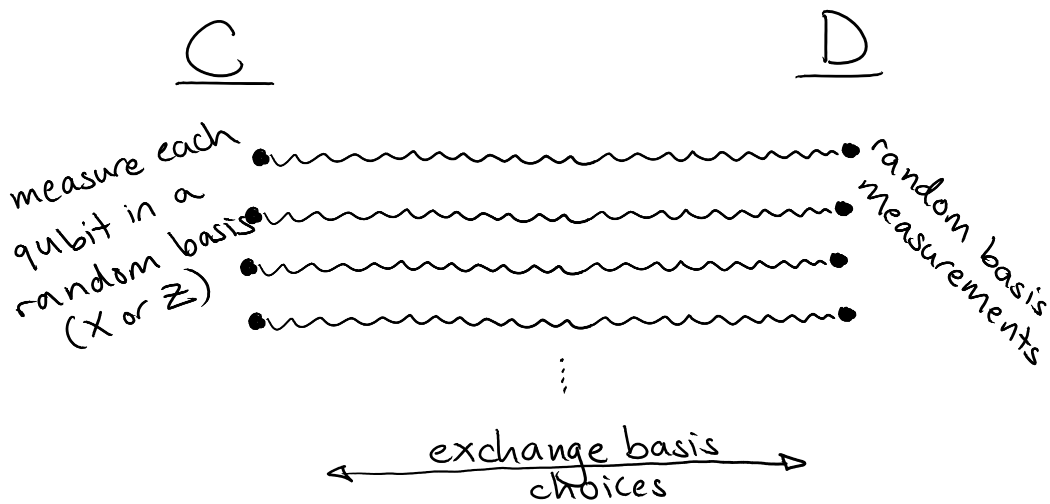
$$\Rightarrow \mathcal{E}^B_{1,j}(\rho_1) \approx \hat{\mathcal{E}}^B_{1,j}(\hat{\rho}_1)$$

since a unitary doesn't change trace distance

Applications:

- "Device-independent" quantum key distribution (DIQKD)

  BB'84-style protocol:



  same basis $\Rightarrow$ should get same result

  Security requires you trust the measurement devices

  Cheating strategy:

  Devices & attacker share strings $x, z \in \{0,1\}^n$

  In game j, output $\begin{cases} x_j & \text{for } X\text{-basis meas.} \\ z_j & \text{for } Z\text{-basis meas.} \end{cases}$

  $\rightarrow$ indistinguishable from the ideal case, but attacker has the key

  Solution: Call the devices Alice & Bob, test them

- A classical party can delegate a quantum computation, and QMIP = MIP*: quantum multi-prover interactive proof systems can be dequantized (next time)

Open questions:

- "Parallel composition" of CHSH games: play the games all at once (see, eg., Kempe-Vidick)

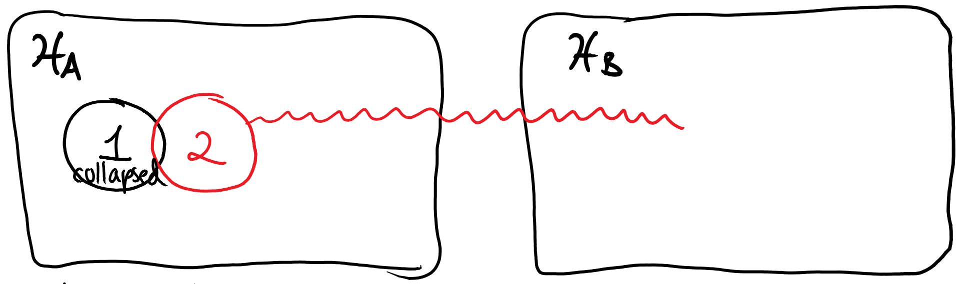
- Generalize to other games
  (for a better understanding, and simpler & more flexible proof)
- Make the test more efficient:
  Can we determine a tensor-product structure even starting with a constant noise rate?
  My guess: yes.

  Possible conjecture:
  For n CHSH games (sequential or parallel),
  If $\mathbb{P}[\text{win } 84\%] \approx 1$,
  then A & B must share $\approx n$ EPR pairs...

- Develop more tools for working with unstructured Hilbert spaces (e.g., de Finetti, information theory)
- Study sequential games with communication between rounds

  - although qubit locations can change, is there still a tensor-product structure?

- More applications
  - Practical device-independent quantum key distribution (DIQKD)
    - better handle noise
    - higher key rate
    - allow entanglement to be generated on the fly
  - Starting with any cryptographic protocol, give it device-independent security
  - Variants of randomness extraction & amplification
  - All sorts of possible extensions to secure delegated quantum computation (next time)



Alice overlapping measurement strategy