Games to establish structure in an unknown Hilbert space

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 
\[ \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \alpha_x |x \rangle \langle y| \]

→ 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**
- Bias in the random bit

**Subtle problems**
- Small correlations between successive runs

**Now you’re just paranoid**
- 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 $AB = 0$, $\frac{3}{4}$ of the time

**Best quantum strategy:**

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

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

If both inputs are 1,

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

⇒ wins $\cos^4 \frac{\pi}{8} \approx 85\%$ 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:** \( \Pr[\text{win}] \geq \cos^2 \frac{\pi}{8} - \epsilon \), then up to local isometries on $\mathcal{H}_A, \mathcal{H}_B$,

- initial state \( \approx (1001 + 1111) \otimes \text{(more)} \)
- effect of Alice & Bob’s measurements on this state \( \approx \) (ideal measurement strategy)

**Proof:**
Two-outcome projective measurement \( \leftrightarrow \) hyperplane

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

**Problem:** How do we know if \( \Pr[\text{win}] \geq \cos^2 \frac{\pi}{8} - \epsilon \)?

**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
  \( \Pr[\text{win} \geq (\omega^* - \epsilon) \cdot 10^6 \text{ games}] \geq 1 - \epsilon \)

\( \Rightarrow \) at the start of a random game, most likely \( \Pr[\text{win that game}] \geq \omega^* - \epsilon' \)
\( \Rightarrow \) Theorem applies
Idea: Repeated CHSH games give a test for quantum devices. But more complex applications require more qubits' worth of entanglement.

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:**

\[
\begin{array}{cccc}
\times \times \times & \times \times \times & \times \times \times & \ldots \\
\text{n games} & \text{n games} & \text{n games} & \text{n games}
\end{array}
\]

- \(N \) blocks of \(n\) sequential CHSH games

- If: \( P[\text{win} > \omega - \epsilon \text{ of games}] \geq 1 - \epsilon \)

- Then: At the beginning of a random block of \(n\) games, Alice & Bob's strategy \( \approx \) ideal strategy \((100) + (111)\)\(\otimes\) for those games 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 = \(\epsilon^\circ\).

**Formally:** \(\approx\) means with super-operators, trace distance

\[
\begin{align*}
\{\Pi, 1-\Pi\} & \quad \rightarrow \quad \text{super-operator} \\
\epsilon(\rho) &= \Pi \rho \Pi \otimes |0\rangle\langle 0| + (1-\Pi) \rho (1-\Pi) \otimes |1\rangle\langle 1|
\end{align*}
\]
Ideal strategy: $\hat{E}_A = \frac{1}{2} \mathbf{1} 0 \otimes \sum_{x=0}^{1} |x\rangle \langle x| \otimes \prod_{x=0}^{\sigma} |x\rangle \langle x| + \frac{1}{2} 1 1 \otimes \prod_{x=0}^{\sigma} |x\rangle \langle x|$

- Input coin $A$
- Projective measurement (depending on $A$)
- Output $X$

"Alice & Bob's strategy for those games (100) + (111) pair $j$ for game $j$ means that up to local isometries $H_A \rightarrow (C^2)^{\otimes n} \otimes H_A'$, $H_B \rightarrow (C^2)^{\otimes n} \otimes H_B'$,\n
$$\left\| \hat{E}_{A,B}^{1,j} (\rho) - \hat{E}_{A,B}^{1,j} (n \text{ EPR pairs}) \right\|_1 \approx 0.$$\n
Joint super-operator for games 1 to $j$.

Proof sketch: 3 steps

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

2. 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?
How do errors accumulate?

a) Small errors away from ideal could slowly move qubits
   
   Example: 5 EPR pairs in tensor product

   \[ \begin{array}{cccc}
   1 & 2 & 3 & 4 \\
   \end{array} \]

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

   \[
   |4\rangle \quad \text{if } \|\Pi 14\| = \frac{1}{\sqrt{3}} + \text{error} \]

   and errors can accumulate quickly!

b) Fixing earlier games breaks later games

Assume: \[ P[\text{win game 1}] > w^* - \epsilon, \]
\[ P[\text{win game 2 | game 1's outcome}] > w^* - \epsilon \]

Then: At B's initial state & measurements are \( \Gamma \)-close to ideal,
At the beginning of game 2, measurements & current state are \( \Gamma \)-close to ideal.

Now fix game 1: Replace with ideal strategy
\[ \Rightarrow P[\text{win game 2 | game 1}] \Rightarrow w^* - \epsilon - \Gamma \]
\[ \Rightarrow \text{new strategy is } \epsilon^\mu \text{-close to ideal} \]

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

slightly overlapping qubits in sequential games
accumulating errors allow for huge overlap later
— no tensor product structure
(If you fix the state at the beginning of game 2, that might not correspond to anything before game 1)

⇒ 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

![Diagram](image)

Formally:

**Assume:** Alice measures a qubit in every game, possibly overlapping

⇒ In game 1, her qubit collapses to \( |1\rangle, |0\rangle, |1\rangle, |+\rangle, \text{or} |1\rangle \)

![Diagram](image)
Add an ancilla $|0\rangle$ qubit, and swap it with game 1’s qubit:

Swap!

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?

Actual strategy (up to isometry)

- play game 1
- apply isometry
- add 10%, rotate
- & swap with game 1

Tensor-product strategy

- apply isometry
- play games 2 to n

Actual strategy

- rotate to $|x_1\rangle$ and swap in
- $|0\rangle$ to $|x_1\rangle$
- qubit for game 2

Tensor-product strategy

- $|x_1\rangle$
- qubit for game 2

These are the same if $|x_1\rangle$ stays collapsed through games 2 to n.
Problem: Strategies ideal together versus separately

We know

\[ \mathcal{E}_{i,j}^A(\rho_\psi) \approx \hat{\mathcal{E}}_{i,j}^A(\hat{\rho}_\psi) \]
\[ \mathcal{E}_{i,j}^B(\rho_\psi) \approx \hat{\mathcal{E}}_{i,j}^B(\hat{\rho}_\psi) \]

\[ \text{actual strategy} \quad \text{ideal strategy} \]
\[ \text{after finishing } j-1 \text{ games} \quad \left[ \rho_\psi = \mathcal{E}_{i,j-1}^{AB}(\rho_i) \right] \]

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

\[ \mathcal{E}_{i,j}^A(\rho_i) \approx \hat{\mathcal{E}}_{i,j}^A(\hat{\rho}_i) \]
\[ \mathcal{E}_{i,j}^B(\rho_i) \approx \hat{\mathcal{E}}_{i,j}^B(\hat{\rho}_i) \]

\[ \text{actual separate strategies} \quad \text{ideal separate strategies} \]

Trick:

Given

\[ \mathcal{E}_{i,j}^A \mathcal{E}_{i,j}^B(\rho_i) \approx \hat{\mathcal{E}}_{i,j}^A \hat{\mathcal{E}}_{i,j}^B(\hat{\rho}_i) \]

\[ \text{actual joint strategy} \quad \text{ideal joint strategy} \]
\[ \text{for } j \text{ games} \]

Observe: After Bob's super-operator,

EPR pairs are collapsed

\[ \Rightarrow \text{Instead of measuring, Alice can just rotate her qubits unitarily} \]
\[ \hat{\mathcal{U}}_{i,j} \mathcal{E}_{i,j}^B(\rho_i) \approx \hat{\mathcal{U}}_{i,j} \hat{\mathcal{E}}_{i,j}^B(\hat{\rho}_i) \]

\[ \Rightarrow \mathcal{E}_{i,j}^B(\rho_i) \approx \hat{\mathcal{E}}_{i,j}^B(\hat{\rho}_i) \]

since a unitary doesn't change trace distance

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

**BS'84-style protocol:**

![Diagram showing quantum key distribution protocol]

```
C ──── random basis measurements ──── D
measure each qubit in a random basis (X or Z)

exchange basis choices

same basis ⇒ should get same result
```

Security requires you trust the measurement devices

**Cheating strategy:**

- Devices & attacker share strings x, z ∈ {0, 1}^n
- In game j, output { x_j for X-basis meas. } for Z-basis meas.

→ 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, e.g., Kempe-Vidick)
• Generalize to other games
  (for a better understanding, and simpler proof)
  & more flexible

• 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 \( P[\text{win } 84\%] \approx 1 \),
  then A \& B must share \( \approx n \) EPR pairs...

• Develop more tools for working with unstructured
  Hilbert spaces (eg., 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)
$\mathcal{H}_A$ 1 collapsed 2

Alice overlapping measurement strategy

$\mathcal{H}_B$