Announcement:
Project suggestions out!
Pick a topic by 11/16
No class Wed 11/11

\[ \text{MIP}^* \geq \text{MIP} \]

Today: An MIP* protocol that requires quantum

Testing results so far:
1) CHSH game / Magic Square

\[ A_0A_1 \otimes I(\psi) \uparrow = \chi_1 A_0 \otimes I(\psi) \]
\[ \exists \tilde{A}_0, \tilde{A}_1, \tilde{A}_0 \tilde{A}_1 = -\tilde{A}_1 \tilde{A}_0 \]

\[ V: \begin{align*}
A_0 & \rightarrow \tilde{A}_0 \\
A_1 & \rightarrow \tilde{A}_1
\end{align*} \]

2) **Classical BLR**

\[ F(a) F(b) = F(a+b) \quad \text{w.h.p.} \quad \forall a, b \in \mathbb{Z}_n \]

\[ \Rightarrow \exists \mathcal{G} \quad \text{s.t.} \quad \mathcal{G}(a) = F(a) \quad \text{w.h.p.} \]

\[ \mathcal{G}(a) \mathcal{G}(b) = \mathcal{G}(a+b) \quad \forall a, b \]

\[ \Rightarrow \forall a, b \]

3) **Quantum - source BLR**

\[ B^a \leftarrow \mathbb{Z}_n \]

\[ \mathbf{E} \left\langle \psi \left| I \otimes B^a B^b B^a+b \right| \psi \right\rangle \geq 1-\varepsilon \]
Consider group generated by tensor products of $I_3 \otimes I_3 \otimes \ldots$

$I \circ I = \pm \times$

$2 \circ I = -I \circ I$: $(I_x)(I_z)(I_x)$

$(I \pm)$
Any element can be written as

\[ P = \prod_{s \in \{0, 1\}^n} X(a) Z(b) \]

\[ X(a) = X^0 \otimes X^1 \otimes X^2 \otimes \ldots \]

Relations:

**BLR** \[ \begin{cases} X(a)X(b) = X(a+b) \\ Z(a)Z(b) = Z(a+b) \end{cases} \]

**CHSH** \[ X(a)Z(b) = (-1)^{a_0 b_0} Z(b)X(a) \]

Goal: Design a test for these relations
The Pauli Braiding Test

3 sub-tests. (Verifier flips a coin and picks a sub-test to execute)

1) BLR: Verifier picks basis \( W \in \{X, Z\} \) at random.

Execute \( 2 \) BLR test + tell provers \( W \) (questions look like \( (W, a, b) \in \{0, 1\} \)

2) Anticommutation test: (CASH)

Verifier pick pair \( a, b \in \{0, 1\} \)

s.t. \( \langle a, b \rangle = 1 \)
Send \((a, b)\) to both parties and play CHSH

(Q's look like \((a, b), 0 \sim 1\)
A's look like \(0/1\))

3) Consistency test:
Verifer pick \((a, b)\) s.t. \((a, b) = 1\)

Send Alice \((a, b)\) and CHSH

Bob gets \#BLR-type \(g\).

\(x = 0\): \(("2", b)\)

\(x = 1\): \(("X", a)\)

Check that Alice's answer = Bob's answer
Alice's subtest 2 measurement is consistent with Bob's subtest 1 measurement.

An optimal strategy:

\[ \omega^*(S_{\text{PB}}) \leq \frac{2}{3} + \frac{1}{3} \cdot \cos^2 \left( \frac{\pi}{8} \right) \]

\[ \omega^*(S^{(2)}) = \omega^*(S^{(3)}) = \cos^2 \left( \frac{\pi}{8} \right) = 1 \]

\[ \omega^*(S^{(3)}) = 1 \]

Strategy:

\[ -|\psi\rangle = |\text{EPR}\rangle \]
- For \((W, a, b)\)
  
  Measure \(W(a)\) and \(W(b)\)
  
  (e.g. measure all qubits in \(W\) basis, compute \(S\) output, evaluate at \(a, b\))

- For \((a, b), x\)

  Alice: If \(x = 0\), measure \(Z(b)\)
  
  If \(x = 1\), measure \(X(a)\)

  Bob: If \(y = 0\), measure \(\frac{Z(b) + X(a)}{\sqrt{2}}\)
  
  If \(y = 1\), measure \(\frac{Z(b) - X(a)}{\sqrt{2}}\)

(Note: unitarily equiv. to standard CAT protocol on qubit 1)
This stat is unique, and PBT is a self-test for it:

**Thm:** Suppose $A \leq B \leq \mathcal{R}$, then

\[ \Pr(\omega^* \geq \epsilon) \leq \epsilon \]  

Then, there exist local isometries $V_A, V_B$ such that

\[ V_A \otimes V_B (|\psi\rangle) \leq \frac{\epsilon}{3^k} \]

Let $M^{\psi_0}$ be the observable used by Alice for $a$ ($W_0 a$)

\[ \mathbb{E}_a \left[ \left| \left| V_A \otimes V_B (M^{\psi_0}) - W(a) \otimes I \right| \right|_{EPR} \right] \leq \frac{\epsilon}{3^k} \]
Proof sketch:

Explicit proof:

\[ MW_{a} \]

CHSH analysis:
- On average are \( a, b \)
\[ M_{X,a} M_{Z,b} = -M_{X,a} M_{Z,b} \Rightarrow \text{exactly anticommuting for each pair } a, b \]

\& BLR analysis:
- \[ M_{X,a} M_{X,b} = M_{X,a+b} \]
\[ \Rightarrow \text{exactly linear } X \text{ measurement} \]
\[ \Rightarrow \text{exactly linear } Z \text{ measurement} \]
Trick:

\[
\frac{1}{2} |EPR^\otimes n\rangle
\]

\[
\tilde{w},a \quad M \quad \tilde{w},q
\]

\[
\tilde{M} = M \otimes W(a) \otimes I
\]

This trick makes everything almost commute

\[
\tilde{M} \tilde{M} \tilde{M} \tilde{M} \tilde{M} \tilde{M} \tilde{M}
\]

\[
\Rightarrow \text{Define "product measurement"}
\]

\[
C(q,b) = \tilde{M} x, a \quad \tilde{M} z, b
\]

\[\leftarrow \text{morally}\]
\[(a, b) \cdot (a', b') = (a+a', b+b') \]

\[\downarrow \text{apply } g\text{BLR} \]

\[\mathcal{F} \quad P(a, b) = C(g, b) \]

\[D(a, b) \cdot D(a', b') = D(a+a', b+b') \]

Define \[P(a, b) = D(a, b) \otimes X(b) \otimes Y(b) \]

2nd half of EPR

\[P \text{ satisfies Pauli group rels} \]

\[P(a, b) \]
Construct a local isometries $V_A$ mapping

$$V_A(M^{w,a}) | \psi \rangle \times W(a) \psi \rangle$$

Slick proof:

Observe that the tensor trick is the Fourier transform over the Pauli group in another guise

[$\text{Gowers Hatami '15}$]

Thm. Suppose $f : \mathbb{Z}_p \rightarrow \mathbb{C}$ s.t.

$$\mathbb{E}_{g,h \in \mathbb{Z}_p} \left\| f(g) \cdot f(h) - f(gh) \right\|_F^2$$
\[ \leq \in \mathbb{C}^n \rightarrow \mathbb{C}^n \]

Then, \( \exists \text{ isometr } V, \; g : G \rightarrow \mathbb{C}^n \)

s.t. \( Vf \mathcal{O} V^+ = g \langle b \rangle \)

\( g \) is an exact representation

\( g(h) \cdot g(h') = g(\chi_{hh'}) \)