6.S979 Lecture 19

Announcement:

Project suggestions out!

Pick a topic by 11/16

No class Wed 11/11

$\mathrm{MIP}^* \supseteq \mathrm{MIP}$

Today: An MIP^* protocol that requires quantum

Testing results so far:

1) CHSH game / Magic Square

$$A_0 A_1 \otimes I |\psi\rangle \approx - A_1 A_0 \otimes I |\psi\rangle$$

$\longrightarrow \exists\ \tilde{A}_0\ \tilde{A}_1,\ \tilde{A}_0\tilde{A}_1 = -\tilde{A}_1\tilde{A}_0$

$V:\ A_0 \xrightarrow{\approx} \tilde{A}_0$

$A_1 \xrightarrow{\approx} \tilde{A}_1$

2) Classical BLR

$F(a)F(b) \underset{\approx}{=} F(a+b)$ w.h.p. $a,b \sim \{0,1\}^n$

$\Rightarrow \exists\ G$ s.t. $G(a) = F(a)$ w.h.p.

$G(a)\,G(b) \underset{\cdot}{=} G(a+b)\ \forall\ \underline{a}\ b$

" $(-1)^{a\cdot u}$

3) Quantum-sound B2R

$B^a \leftarrow \{0,1\}^n$

$\mathop{\mathbb{E}}_{a,b} \langle\psi| I \otimes B^a B^b B^{a+b} |\psi\rangle \geq 1-\varepsilon$

$$\Downarrow$$

$$\exists\ \mathcal{B}^a, \quad \mathcal{B}^a|\psi\rangle \approx B^a|\psi\rangle$$

$$\mathcal{B}^a\mathcal{B}^b = \mathcal{B}^{a+b}$$

$$\left(\mathcal{B}^a = \sum (-1)^{\langle a,u\rangle} M^u\right)$$

Pauli ("Weyl-Heisenberg") group <u>on n qubits</u>:

n qubits (state space $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$)

Consider group generated by tensor products of I, X, Z

$I \otimes I \qquad I \otimes X$

$Z \otimes I \qquad -I \otimes I = (IX)(IZ)(IX)(IZ)$

Any element can be written as

$$P = (-1)^s X(a) Z(b)$$

$a, b \in \{0,1\}^n$

$$X(a) = X^{a_0} \otimes X^{a_1} \otimes X^{a_2} \otimes \cdots$$

Relations:

BLR
$$\begin{cases} X(a)X(b) = X(a+b) \\ Z(a)Z(b) = Z(a+b) \end{cases}$$

CHSH
$$X(a)Z(b) = (-1)^{\langle a,b\rangle} Z(b)X(a)$$

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) <u>BLR:</u> Verifier picks basis $W \in \{X, Z\}$ at random.

Execute $\mathbb{Z}_2$BLR test + tell provers W (questions look like (W, a, b) $\in \{0,1\}^n$?

answers are in $\{0,1\}$ or $\{0,1\}^2$)

2) Anticommutation test: (CASH)

Verifier pick pair $a, b \in \{0,1\}^n$ s.t. $\langle a, b \rangle = 1$

Send (a,b) to both parties
and play CHSH
(Q's look like $((a,b), 0 \text{ or } 1)$
A's look like $0/1$)

3) Consistency test:
Verifier pick (a,b) s.t. $\langle a,b\rangle = 1$

Send Alice (a,b) and CHSH q.
$x \in \{0,1\}$

Bob gets qBLR-type q.
$x=0$: ("Z", b)

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

Check that Alice's answer
= Bob's answer

$\Rightarrow$ Alice's subtest 2 measurement is consistent w/ Bob's subtest 1 measurement

- - - - - - - - - - - -

An optimal strategy:

Obs: $\omega^*(G_{SPBT}) \leq \frac{2}{3} + \frac{1}{3} \cdot \cos^2(\pi/8)$

$$\omega^*(G^{(2)}) = \omega^*(CHSH) = \cos^2(\pi/8)$$
$$\omega^*(G^{(1)}) = 1$$
$$\omega^*(G^{(3)}) = 1$$

Strategy:

- $|\psi\rangle = |EPR\rangle^{\otimes n}$

- For $(W, a, b^?)$

Measure $W(a)^{✓}$ and $W(b)^{✓}$

(e.g. measure all qubits in W basis, compute $\mathcal{E}_H$ 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 CHSH strat. on qubit 1)

This strat is unique, and PBT is a self-test for it:

Thm: Suppose A & B win w/ prob $\omega^* - \varepsilon$. Then, $\exists$ local isometries V_A, V_B s.t.

no n

$$V_A \otimes V_B (|\psi\rangle) \underset{\varepsilon^{1/4}}{\approx} |EPR^{\otimes n}\rangle |aux\rangle$$

Let $M^{W,a}$ be the observable used by Alice for a (W, a)

$$\mathop{\mathbb{E}}_{a} \left\| V_A \otimes V_B (M^{W,a} \otimes I |\psi\rangle) - W(a) \otimes I |EPR^{\otimes m}\rangle |aux\rangle \right\|^2 \le \varepsilon^c$$

no n

Proof sketch:

Explicit proof:

$M^{W,a}$

CHSH analysis:

- on average over a, b

$$M^{X,a} M^{Z,b} \hat{\approx} -M^{Z,b} M^{X,a}$$

$\Rightarrow$ exactly anticommuting for each pair a,b

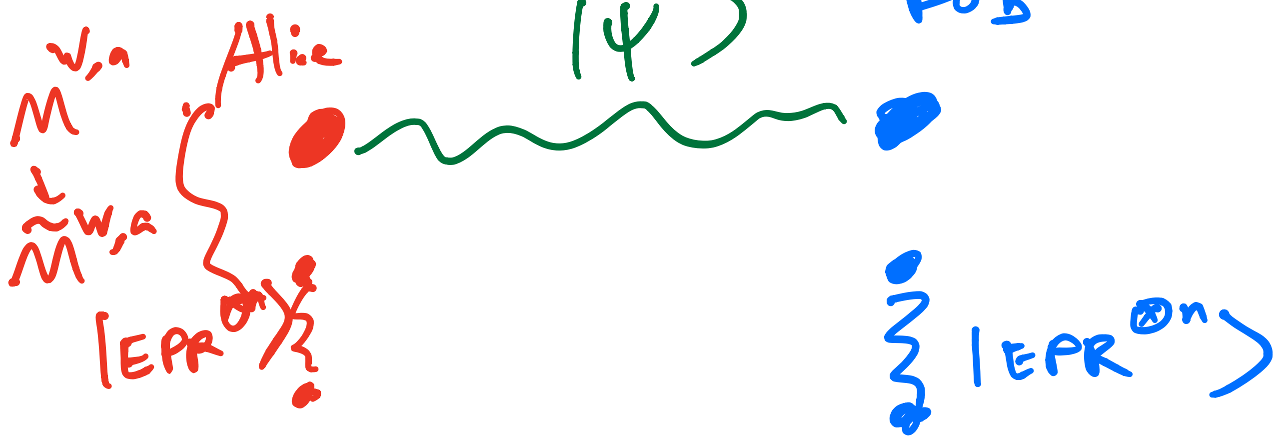
BLR analysis:

- $M^{X,a} M^{X,b} \hat{\approx} M^{X,a+b}$

$\rightarrow$ exactly linear X measurement

$\rightarrow$ exactly linear Z measurement

Trick:



$$\tilde{M}^{W,a} = M^{W,a} \otimes \underbrace{W(a) \otimes I}_{\text{private EPR pairs}}$$

This trick makes everything almost commute

$$\tilde{M}^{X,a}\,\tilde{M}^{Z,b} \approx \tilde{M}^{Z,b}\,\tilde{M}^{X,a}$$

$\Rightarrow$ Define "product measurement"

$$C(a,b) = \tilde{M}^{X,a}\,\tilde{M}^{Z,b}$$

← morally

$$C(a,b)\,C(a',b') \approx C(a+a',\, b+b')$$

$$\Big\Downarrow \text{ apply qBLR}$$

$$\exists\, D(a,b) \approx C(a,b)$$

$$D(a,b)\,D(a',b') = D(a+a',\, b+b')$$

Define $P(a,b) = D(a,b) \otimes \widetilde{X(a)Z(b)}$

2nd half of EPR

P satisfies exactly Pauli group rels

$\Longrightarrow$ Construct a local isometry V_A mapping

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

Slick proof:

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

[Gowers Hatami '15]

Thm: Suppose $f: G \to U(n)$ (G group)

s.t. $\mathbb{E}_{g,h \in G} \| f(g) \cdot f(h) - f(gh) \|_F^2$

$\leq \varepsilon$

Then, $\exists$ isomets $V: \mathbb{C}^n \to \mathbb{C}^{n'}$, $g: G \to U(n')$

s.t. $V f(h) V^\dagger \approx g(h)$

g is an exact representation

$g(h) \cdot g(h') = g(hh')$