Remainder: Pet 2 on Friday  
Project info up by Friday (read a paper (or a few) and summarize)

---

Last time:
Quantum: sound locally testable code

![Diagram](A \rightarrow i \rightarrow B \rightarrow i \leftarrow b \rightarrow V)

If $A \& B$ pass the test w/ prob $1 - \varepsilon$, then

$\exists \varepsilon M^{x^3} \text{ data to be encoded}$

$s.t.
\Theta B_b(1^4) \times \sum_{i \in 0} M^{x^4} \\
| x : 3(x) = b$

$\delta(\varepsilon)$
Reminder: Use $x^*$ to obtain an assignment for the CSP

$A \rightarrow B$

strat in $G_{CSP}$

Thm: Hadamard code is $g$-sound LTC test is the BLR test

$(f(x) + f(y)) \equiv f(x+y)$

$g, a'$

$g, b$

$g, a$ or $x+y$

$g, b = a'$

$g, a = b$

$g, a = a + a'$

A & B use the same function/encoder
Thm restated: If $A < B$ pass test $\sim p$ub. $1 - \varepsilon$, $\exists M^x$

s.t. $\sum_{\text{obs}} B_0^x \downarrow \sum_{\text{obs}} M^u$

$u : \exists (u) \sum = b$

$\langle u, z \rangle = b$

\[ \ \]

Pf: Define observables

$B^2 := B_0^2 - B_1^2$

(\text{analogous to } F(2) \in \mathcal{F}_{\varepsilon, 13})$

Define Fourier transform

$\hat{B} u := \mathcal{F}(x) u \Rightarrow \hat{B} x$

$\hat{B} x = \sum_{u} \langle x, u \rangle \hat{B} u$

Plancherel theorem

$\sum_{u} (\hat{B} u)^2 = I = \mathcal{F}(B^x)^2$
\[ \text{Prob} \left[ A, B \text{ win} \right] \geq 1 - \varepsilon \]

\[ \implies \exists \sum \frac{\left( F_{\text{win}} \right)^{3}}{n} \geq 1 - 2\varepsilon \]

\[ \exists \frac{\left( F_{\text{win}} \right)^{2}}{n} = 1 \implies \exists u, \tilde{F}_{u} \text{ is large} \]

\[ \implies \tilde{F}_{u} \in \left( F_{\text{win}} \right) \]

Observe:

\[ C_{u} := (B_{u}) \quad \text{Hamilton, PSD matrix} \]

\[ \sum_{u} C_{u} = I \]

This means \( C_{u} \) is almost a projective \( \delta \)-measure

\[ u \neq v \quad C_{u} \cdot C_{v} = 0 \quad \left( C_{u}^{2} \right) = C_{u} \]
Wishful thinking: Suppose \( \exists C^u \) is a proj. measurement
\[ u \in \mathcal{E}_{\text{0,13}}^n \]

Let's take \( C^u \) to be our \( M^u \)

Need to show that
\[ I \otimes B_{\text{14}}^z \leq \sum_{u \in \mathcal{E}_{\text{0,13}}^n} I \otimes C^u \]

\[ \exists C^u \ldots I \text{ observable.} \]

\[ I \otimes B_{\text{14}}^z \leq \sum_{u \in \mathcal{E}_{\text{0,13}}^n} (-1)^u I \otimes C^u_1 \]

\[ B_{\text{14}}^z = \sum_{u \in \mathcal{E}_{\text{0,13}}^n} C^u_1 \]

\[ \mathbb{E} \left[ \left\| I \otimes B_{\text{14}}^z - I \otimes \sum_{u \in \mathcal{E}_{\text{0,13}}^n} C^u_1 \right\|^2 \right] \]

(Classically: \( \mathbb{E} \left[ F(z) - G(z) \right]^2 \leq \sigma \))

\[ = \mathbb{E} \left( 2 - \langle \psi | I \otimes B_{\text{14}}^z B_{\text{14}}^z | \psi \rangle \right) \]
\[-\langle 41 \circ \beta^2 \bar{B}^2 14 \rangle \]

\[= 2 - 2 \text{Re} \left\langle 41 \circ \beta^2 \bar{B}^2 14 \right\rangle \]

\[= 2 - 2 \text{Re} \left\langle 41 \circ \beta^2 \bar{B}^2 \frac{\tilde{u}^3}{u} \right\rangle \]

\[\leq 2 - 2 \text{Re} \left\langle 41 \circ \beta^2 \bar{B}^2 \frac{\tilde{u}^3}{u} \right\rangle \]

\[\leq O(\sqrt{3}) \]

So \( C^u := (\tilde{B}^u)^2 \) is the measurement \( M^u \) we wanted.
Except $c^n$ is not a (proj.) measurement.

To fix this, use the Naimark dilation thm

**Thm:** Suppose you have $\Sigma c^n \in \mathcal{B}$ on $\mathcal{H}$

$c^n \geq 0$, $\Sigma c^n = I$

Then, $\exists \ D^n$ on $\mathcal{H} \oplus \mathcal{H}_{aux}$ s.t.

$D^n \geq 0$, $(D^n)^2 = D^n$, $\Sigma D^n = I$

$D^n D^v = 0$ for $u \neq v$

$$D^n = \begin{pmatrix} c^n & \cdots \\ \vdots & \ddots \end{pmatrix} \iff (\mathcal{I} \otimes \mathcal{D}_{aux}) D^{\ast} (\mathcal{I} \otimes \mathcal{D}_{aux}) = c^n$$
This implies that

\[ P_{\text{C}}(\psi) = \langle \psi \mid C^n \mid \psi \rangle = \langle \psi \mid \text{col}_{\text{aux}} D^u \mid \psi \rangle_{\text{aux}} \]

\[(\ast) \quad \langle \psi \mid M \cdot C^n \mid \psi \rangle = \langle \psi \mid \text{col} (\text{M} \otimes I) D^u \mid \psi \rangle_{\text{aux}} \]

i.e. you can simulate \( C^n \) w/ prog. measurement.

Things like \( C^n \) are called POVMs.

(For a proj. measurement, \( |\psi\rangle \rightarrow \frac{D^u |\psi\rangle}{\|D^u |\psi\rangle\|} \))

For a POVM, \( |\psi\rangle \rightarrow U_{\text{POVM}} C^n |\psi\rangle \)

\[ \langle x^{(n)} \rangle \langle y \mid B^x C^n \mid y \rangle = \langle y \mid \text{col} (\text{B} \otimes I) D^u \mid y \rangle \]

\[ \langle x^{(n)} \rangle \begin{array}{c}
\| \text{by (\ast)} \| \rightarrow \\
\langle y \mid \text{col} (\text{M} \otimes I) D^u \mid y \rangle \end{array} \]
We showed that Hadamard code is quantum sound

\[ \equiv \text{the protocol for encoded QMD, e.g. } \text{works for MIP}^* \]

\[ \text{NP} \subseteq \text{MIP}^* [\text{poly}(n) \text{ messages}] \]

Turns out that the multilinearizty code is also \text{Q}-sound

(special case of low degree code)

polynomial is multivariate

w/ individual degree \( \leq 1 \)

\[ \text{NEXP} \subseteq \text{MIP}^* [\text{poly}(n) \text{ messages}] \]

Ito, Vidick '12 [also showed quantum soundness of BLR]
\[ \text{NEXP} = \text{MIP} \]
\[ \text{MIP} \leq \text{MIP}^* \]

---

So far, we showed that classical protocols for classical problems can be made sound against entanglement.

(Obs: you can pass the qq. BZR test without any entanglement.)

Q: Can we design protocols where honest provers need entanglement?  
\( \text{(MIP} \not\leq \text{MIP}^*) \)
Idea: Combine BLR w/ self-testing to design a self-test for many EPR pairs.

**Pauli Braiding Test:**

Recall that q. analysis of BLR constructed $B^Z = \mathbb{Z}_2 \times \{+1\} D^n$.

$B^Z \otimes B^Z$ observables,

$[B^Z, B^{Z'}] = 0$ commutation

$B^Z \cdot B^{Z'} = B^{Z+Z'}$ group relations $\mathbb{Z}_2^n$ linear relation

Recall the CHSH game:

$A_0, A_1, B_0, B_1 \quad B_0 \times B_0, B_1 \times B_1$

$B_0, B_1 = -B_0, B_0$ relation of Pauli group.
Idea: Combine BLR + CHSH to test the relations satisfied by Pauli matrices on \( n \) qubits.

\[
X^a = X^{a_1} \otimes X^{a_2} \otimes \ldots \otimes X^{a_n}
\]

\[
\mathbb{Z}^b = \mathbb{Z}^{b_1} \otimes \mathbb{Z}^{b_2} \otimes \ldots \otimes \mathbb{Z}^{b_n}
\]

\[
\begin{align*}
IX &= X^{01} \\
XX &= X^{11}
\end{align*}
\]

\[
X^a X^b = X^{a+b \mod 2}
\]

\[
\mathbb{Z}^a \mathbb{Z}^b = \mathbb{Z}^{a+b \mod 2}
\]

\[
X^a \mathbb{Z}^b \mathbb{Z}^c = (a,b,c)\mathbb{Z}^a \\
X^a \mathbb{Z}^b = (a,b)\mathbb{Z}^a
\]