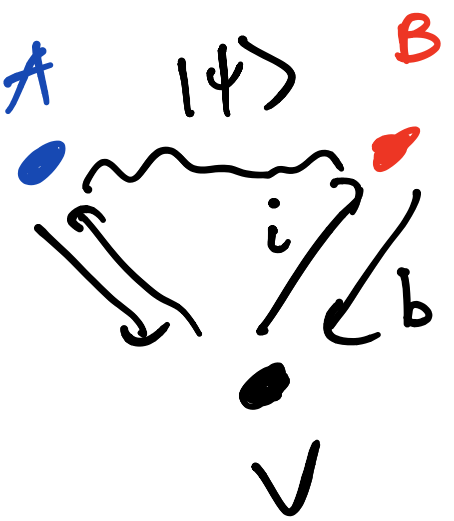
6.S979 Lecture 18

- Reminder: Pset 2 on Friday
- Project info up by Friday (read a paper (or a few) and summarize)

Last time:

Quantum-sound locally testable code



B^i_b

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

$\exists \{M^x\}_x$ ← data to be encoded

s.t. $I \otimes B^i_b|\psi\rangle \underset{\delta(\varepsilon)}{\approx} \sum_{x : E(x)_i = b} I \otimes M^x |\psi\rangle$

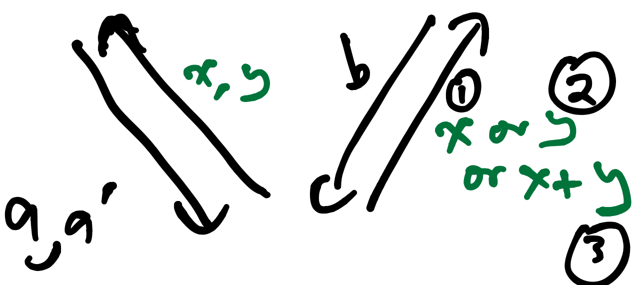
Reminder: q-sound LTC solve the Clause Variable game

Use M^x to obtain an assignment for the CSP

$$\underset{\text{strat in } G_{CV}}{A \ |\phi\rangle \ B} \xrightarrow{\ M^x\ } x \text{ assignment for } \Phi$$

Thm: Hadamard code is q-sound LTC
test is the BLR test

$\left(f(x) + f(y) \stackrel{?}{=} f(x+y)\right)$



① $a \stackrel{?}{=} b$

② $b \stackrel{?}{=} a'$

③ $b \stackrel{?}{=} a + a'$

i.e. A & B use the same function/codeword

Thm restated: If A & B pass test w/ prob. $1-\varepsilon$, $\exists$ M^x s.t. $I \otimes B^z_b \approx \sum_{u : \{(u)_H\}_z = b} I \otimes M^u$

$\langle u, z \rangle = b$

Pf: Define observables

$$B^z := B^z_0 - B^z_1$$

(analogous to $F(z) \in \{\pm 1\}$)

Defined fourier transform

$$\text{Hermitian} \rightarrow \hat{B}^u := \mathbb{E}_x (-1)^{\langle x, u \rangle} B^x \qquad x \in \{0,1\}^n$$

$$B^x = \sum_u (-1)^{\langle x, u \rangle} \hat{B}^u$$

Plancherel theorem

$$\sum_u (\hat{B}^u)^2 = I = \mathbb{E}_x (B^x)^2$$

$\mathrm{Prob}[A, B \text{ win}] \geq 1 - \varepsilon$

$$\Rightarrow \sum_u \langle \psi | I \otimes (\hat{B}^u)^3 | \psi \rangle \geq 1 - \underset{\sim}{O(\sqrt{\varepsilon})}$$

$$\left(\sum_u (\hat{F}^u)^3 \geq 1 - 2\varepsilon \right.$$

$\sum_u (\hat{F}^u)^2 = 1 \Rightarrow \exists u, \hat{F}^u$ is large

$\left. \Rightarrow F \approx (-1)^{\langle x, u \rangle} \right)$

Observe:

$c^u := (\hat{B}^u)^2 \leftarrow$ Hermitian, PSD matrix

$$\sum_u c^u = I$$

This means c^u is <u>almost</u> a $\overbrace{\text{projective}}$ g. measurement

$u \neq v \quad c^u \cdot c^v = 0, \quad (c^u)^2 = c^u$

Wishful thinking: Suppose $\{C^u\}$ is a proj. measurement

$u \in \{0,1\}^n$

Let's take C^u to be our M^u

Need to show that

$$I \otimes B^z_b |\psi\rangle \approx \sum_{u : \langle u, z\rangle = b} I \otimes C^u |\psi\rangle$$

$\sum_b (-1)^b \ldots$ $\updownarrow$ observable.

$$I \otimes B^z |\psi\rangle \approx \sum_u (-1)^{\langle u,z\rangle} I \otimes C^u |\psi\rangle$$

$\mathcal{B}^z = \sum_u (-1)^{\langle u,z\rangle} C^u$

$$\mathop{\mathbb{E}}_z \left\| I \otimes B^z |\psi\rangle - I \otimes \underbrace{\sum_u (-1)^{\langle u,z\rangle} C^u}_{} |\psi\rangle \right\|^2$$

(Classically: $\mathop{\mathbb{E}}_z [F(z) - G(z)] \leq \text{small}$)

$$= \mathop{\mathbb{E}}_z \left(2 - \langle\psi| I \otimes B^z \mathcal{B}^z |\psi\rangle \right.$$

$$- \langle \psi | I \otimes \mathcal{B}^z B^z | \psi \rangle \Big)$$

$$= 2 - 2\,\mathrm{Re} \mathop{\mathbb{E}}_{z} \langle \psi | I \otimes B^z \mathcal{B}^z | \psi \rangle$$

$$= 2 - 2\,\mathrm{Re} \mathop{\mathbb{E}}_{z} \langle \psi | I \otimes B^z \sum_u (-1)^{\langle u, z \rangle} C^u | \psi \rangle$$

$$= 2 - 2\,\mathrm{Re} \mathop{\mathbb{E}}_{z} \sum_u \langle \psi | I \otimes (-1)^{\langle u, z \rangle} B^z \cdot (\hat{B}^u)^2 | \psi \rangle$$

$$= 2 - 2\,\mathrm{Re} \sum_u \langle \psi | I \otimes \hat{B}^u \cdot (\hat{B}^u)^2 | \psi \rangle$$

$$= 2 - 2 \sum_u \langle \psi | I \otimes (\hat{B}^u)^3 | \psi \rangle$$

$$\leq O(\sqrt{\varepsilon})$$

So $C^u := (\hat{B}^u)^2$ is the measurement M^u we wanted

Except C^u is not a (proj.) measurement

To fix this, use the

Naimark dilation thm

Thm: Suppose you have $\{C^u\}$ on $\mathcal{H}$

$C^u \succeq 0$, $\sum C^u = I$

Then, $\exists$ D^u on $\mathcal{H} \otimes \mathcal{H}_{aux}$

s.t. $D^u \succeq 0$, $(D^u)^2 = D^u$, $\sum D^u = I$

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

$$D^u = \begin{array}{cc} & |0\rangle_{aux} \\ |0\rangle_{aux} & \begin{pmatrix} C^u & \cdot & \cdots \\ \cdot & \cdot & \ddots \\ \vdots & & \ddots \end{pmatrix} \end{array} \Leftrightarrow (I \otimes \langle 0|_{aux}) D^u (I \otimes |0\rangle_{aux}) = C^u$$

This implies that

$$\Pr(u) = \langle \psi | C^u | \psi \rangle = \langle \psi | \langle 0 |_{aux} D^u | \psi \rangle | 0 \rangle_{aux}$$

$$(*) \quad \langle \psi | M \cdot C^u | \psi \rangle = \langle \psi | \langle 0 |_{aux} (M \otimes I) D^u | \psi \rangle | 0 \rangle_{aux}$$

i.e. you can simulate C^u w/ proj. measurement

Things like C^u are called POVMs

(for a proj. measurement, $|\psi\rangle \longrightarrow \dfrac{D^u |\psi\rangle}{\| D^u |\psi\rangle \|}$

for a POVM, $|\psi\rangle \longrightarrow \dfrac{U \sqrt{C^u} |\psi\rangle}{\cdots\cdots}$

$$\mathop{\mathbb{E}}_{x} (-1)^{\langle x, u \rangle} \langle \psi | B^x C^u | \psi \rangle = \langle \psi | (\hat{B}^{u3}) | \psi \rangle$$

$\|$ by $(*)$ $\quad /\!/$

$$\mathop{\mathbb{E}}_{x} (-1)^{\langle x, u \rangle} \langle \psi | \langle 0 | (B^x \otimes I) D^u | \psi \rangle | 0 \rangle$$

$B \quad x^i \quad D$

We showed that Hadamard code is quantum sound

$\Rightarrow$ the protocol for encoded quad. eq. works for MIP^*

$NP \subseteq MIP^*$ [poly(n) messages]

Turns out that the multilinearity code is also q-sound
(special case of low degree code)
polynomial is multivariate w/ individual degree 1)

$NEXP \subseteq MIP^*$ [poly(n) messages]

Ito Vidick '12 [also showed quantum soundness of BLR]

$$NEXP = MIP$$

$$MIP \subseteq MIP^*$$

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

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

Q: Can we design protocols where honest provers need entanglement?

$$\left(MIP \overset{?}{\subsetneq} MIP^* \right)$$

Idea: Combine BLR w/ self-testing to design a self-test for <u>many</u> EPR pairs

Pauli Braiding Test:

Recall that q. analysis of BLR constructed $\mathcal{B}^z = \sum (-1)^{\langle y, z\rangle} D^y$

observables

$$B^z_{\otimes I} \approx \mathcal{B}^z$$

commutation

$$[\mathcal{B}^z, \mathcal{B}^{z'}] = 0$$

$(\mathcal{B}^z)^2 = I$

$$\mathcal{B}^z \cdot \mathcal{B}^{z'} = \mathcal{B}^{z+z'}$$

group relations $\mathbb{Z}_2^n$

linearity relation

Recall the CHSH game:

A_0, A_1, B_0, B_1 $\qquad B_0 \approx \mathcal{B}_0 \qquad B_1 \approx \mathcal{B}_1$

$$\mathcal{B}_0 \mathcal{B}_1 = -\mathcal{B}_1 \mathcal{B}_0$$

relation of Pauli group

Idea: Combine BLR + CHSH to test the relations satisfied by Pauli matrices on n qubits

$$X^{a \in \{0,1\}^n} = X^{a_1} \otimes X^{a_2} \otimes \dots \otimes X^{a_n}$$

$$Z^{b} = Z^{b_1} \otimes Z^{b_2} \otimes \dots \otimes Z^{b_n}$$

$IX = X^{01}$

$XX = X^{11}$

$$X^a X^b = X^{a+b} \leftarrow \text{mod } 2$$

$$Z^a Z^b = Z^{a+b} \leftarrow \text{mod } 2$$

$$X^a \cdot Z^b = (-1)^{(a,\cdot b)} Z^b X^a$$