6.5779 Lecture 5

**Theorem (Last time)**:
If a state \( S = \langle 14 \rangle_{A_{1}B_{1}} \) wins CHSH w/ qwb. \( \omega^\text{CHSH} = \frac{3}{2} \)
then \( \exists \) local isometries \( V_A, V_B \)

\[
\| (V_A \otimes V_B) 14 \rangle - 1_{\text{EPR}} \|_{\text{aux}} \|^2 \leq O(\varepsilon^\frac{3}{2})
\]

\[
\| (V_A \otimes V_B) (A_0 \otimes I) 14 \rangle - (Z_0 I_{\text{EPR}}) \|_{\text{aux}} \|^2 \leq O(\varepsilon^{\frac{3}{2}})
\]

"Robust self-testing"

Self-testing more generally:
- We can self-test arbitrary bipartite \( 14 \rangle_{AB} \), but not very robustly
  (Coladangelo, Goh, Scarani)
  \( \varepsilon - \text{close} \Rightarrow \varepsilon \cdot \text{poly}(d) \text{ close to } 14 \)
We can self-test many copies of (EPR)
Can self-test some multipartite states too (e.g. GHZ)
Self-testing arbitrary measurement?
Perfect completeness? (which states)
Robustness for general states
Are generic games self-tests?
(3 examples with non-unique q. strategy)

Another caveat: Self-testing is about the “nearby optimal” regime
0.854 - ε

What about \( \frac{3}{4} + \varepsilon \)
Kamienek: 19?
\[ N \approx 0.764 \Rightarrow \text{some overlap} \]
\[ \leq 0.756 \Rightarrow \text{no self-testing} \]

Valcarce et al. '20

Today: applications of CHSH game (\& self-testing)

#1: Quantum key distribution (QKD)

Bennett & Brassard '84 BB84

Goal: Alice & Bob want to generate a shared private random string "key"

Private quantum channel
Public classical channel
1. Alice \[ \rightarrow \] Bob
   - X \[ \rightarrow \] \[ \begin{array}{c} |1\rangle \rightarrow |-1\rangle \rightarrow |0\rangle \rightarrow |1\rangle \end{array} \]

2. Alice reveals basis settings
   - Bob reveals basis settings

3. Out of rounds / same basis
   - Alice reveals state for \( |a\rangle \) of them

4. Use the other \( |a\rangle \) for your key

This is secure if Alice's and Bob's devices are not faulty

**Attack: Photon number splitting!**

In real world, Alice's qubits are photons
Photon source sometimes generates extra photon

Eve collects extra photons and can learn key

"Device independent security"

Ekert '91

1. Alice  Bob

\[ \frac{x^2 + y^2}{2} \]

2. Reveal bases

3. Pick a fraction of rounds and test CHSH

4. Out of remaining rounds equal bases \(\Rightarrow\) key
"Device-independent security proof"

Success in CHSH rounds

\[ | \Psi \rangle_{AB} \sim | \text{EPR} \rangle_{AB} \perp \text{aux} \]

\[ | \Psi \rangle_{ABE} \sim | \text{EPR} \rangle_{AB} \otimes | \text{joint} \rangle_{ABE} \]

\[ \downarrow \]

Eve's measurement outcomes are uncorrelated w/ Alice & Bob's

"Monogamy of entanglement"
If A is highly entangled w/ B, then AB has low entanglement w/ everyone else
History:
- Ebert '91
- Mayers Yao 98
  introduced “self-testing” to quantum
- Vazirani & Vidick 12
  Play m rounds, can get 0.014m bits of key

What did entanglement buy us?
- Certifiable $\leq$ CHSH
- Private $\leq$ “monogamy”

Application #2:
Randomness expansion
random seed $\epsilon S, 13^n \rightarrow$ Rand expansion \rightarrow random string $\epsilon S, 13^n$

Classically: "pseudorandom generators"

Quantumly: Inherent randomness exists

CFSH $\rightarrow$ certifiable randomness

Roger Colbeck '06 $n \rightarrow k n$
Colbeck & Kent '09
Pironio et al. '10 $n \rightarrow O(n^2)$
Vazirani Vidick '12 $n \rightarrow 2^n$
Miller Shi '14

seed s
In ideal strat $14 \rightarrow$ $\rightarrow 3 + \ldots$ random bits out

To get more expansion

$S \rightarrow$ PRG

2 random bits in $\rightarrow$ 3 random bits out
Upper bound:
Coudron Vien Yuen
"non-adaptive" can expand at most $2^n$

With adaptivity, get infinite randomness expansion!
Coudron Yuen '14
Vics self-testing 8 parties
Chung Shi Wu 4 parties
2 parties is open?

Noise-tolerant version?
Tolerant to realistic noise
General problem w/ self-testing

Other applications:
Self-testing is a "leash" on quantum devices
Delegated GC
Reichardt Unser Vazirani
- Serial repetition of CHSH
- Delegate a quantum circuit of size \( n \) using \( n8000 \) bits of communication

"Verifier on a leash"
Coladangelo Grolla Jeffrie Vidick '16

- Use a generalization of CHSH called Pauli Braiding Test
  Delegate size \( n \) circuit \( n/\ln\ln n \) resources

- Understanding "quantum correlations"
  Interactive proofs - quantum provers
Next time:
Detour to Magic Square game
Contextuality