Lecture 6

Oct 15, 2024

Today:

Proof of uniqueness for CHSH strategy.

Certifiable randomness generation

Errata: I said $\mathcal{O} = \sum_j \omega^j |\psi_j\rangle\langle\psi_j|$ and ω = root of unity is called an observable. That was incorrect. An observable is a Hermitian operator, so it should be defined for real eigenvalues only.

Last time:

$$CHSH = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$$

$$CHSH^2 = 4\mathbb{1} + [A_0, A_1] \otimes [B_0, B_1]$$

we showed that given $A_0^2 = A_1^2 = B_0^2 = B_1^2$ then $\|CHSH\|_{op} \leq 2\sqrt{2}$.

Also $\|CHSH\|_{op} = 2\sqrt{2}$ iff $\|[A_0, A_1]\|_{op} = \|[B_0, B_1]\|_{op} = 2$.

And $\Pr[\text{win}] = \frac{1}{2} + \frac{1}{8} \operatorname{tr}(CHSH\, \rho_{AB})$.

Today:

Let's observe that $\rho_{AB} = \sum_r p_r |\psi_r\rangle\langle\psi_r|_{AB}$

so then $\mathrm{tr}(\mathrm{CHSH}\, \rho_{AB}) = \sum_r p_r \langle \psi_r | \mathrm{CHSH} | \psi_r \rangle$.

Since $\|\mathrm{CHSH}\| \leq 2\sqrt{2} \Rightarrow$ for every r, $|\psi_r\rangle$ is a $2\sqrt{2}$ eigenvector.

So, let's first consider pure strategies $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$ and then come back to mixed strategies.

$$\mathrm{CHSH}\,|\psi\rangle = 2\sqrt{2}\,|\psi\rangle \Rightarrow [A_0, A_1] \otimes [B_0, B_1]\,|\psi\rangle = 4\,|\psi\rangle.$$

Since $\|[A_0, A_1]\|, \|[B_0, B_1]\| \leq 2$, then $|\psi\rangle$ is a ± 2- eigenvector of $[A_0, A_1]$.

Note we are ignoring a $\otimes \mathbb{1}_B$ term everywhere as $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.

<u>Claim</u> A_0, A_1 anti-commute w.r.t. $|\psi\rangle$.

meaning $A_0 A_1 |\psi\rangle = -A_1 A_0 |\psi\rangle$ but $A_0 A_1$ may not equal $-A_1 A_0$ everywhere.

<u>Ex.</u> $$A = \begin{pmatrix} \boxed{Z} & \\ & \boxed{1} \end{pmatrix} \qquad A' = \begin{pmatrix} \boxed{X} & \\ & \boxed{1} \end{pmatrix}$$

then A, A' anticommute w.r.t. any vector $\begin{pmatrix} \alpha \\ \beta \\ 0 \end{pmatrix}$ but do not anticommute for all vectors.

The claim is the best we can hope for. We are using CHSH game to characterize the state of Alice's computer. However, we can only characterize the part of the computer corresponding to the game. How it behaves on the rest of the space we don't know.

<u>Pf of claim</u>

$$(A_0A_1 - A_1A_0)|\psi\rangle = \pm 2|\psi\rangle$$

$$\Rightarrow \quad A_0A_1|\psi\rangle = -A_1A_0|\psi\rangle = \pm|\psi\rangle \text{ since } \|A_0A_1\|, \|A_1A_0\| \leq 1.$$

$$\Rightarrow \quad \underbrace{(A_0A_1 + A_1A_0)}_{\{A_0,A_1\}}|\psi\rangle = 0$$

"anticommutator"

Let S be the nullspace of $\{A_0, A_1\}$.

Notice, $|\tau\rangle \in S \Rightarrow A_0|\tau\rangle \in S$.

$$\begin{aligned}(A_0A_1 + A_1A_0)A_0|\tau\rangle &= A_0A_1A_0|\tau\rangle + A_1|\tau\rangle \\ &= -A_0A_0A_1|\tau\rangle + A_1|\tau\rangle \\ &= (-A_1 + A_1)|\tau\rangle = 0.\end{aligned}$$

Similarly, $A_1|\tau\rangle \in S$.

We've identified that A_0, A_1 are block diagonal w.r.t.

$$\mathcal{H}_A = S \oplus \bar{S},$$

$$A_0 = \begin{pmatrix} \boxed{A_0|_S} & \\ & \boxed{A_0|_{\bar{S}}} \end{pmatrix} \qquad A_1 = \begin{pmatrix} \boxed{A_1|_S} & \\ & \boxed{A_1|_{\bar{S}}} \end{pmatrix}$$

Notice, by definition, $A_0|_S$ and $A_1|_S$ must anticommute.

S is precisely the anticommutation subspace.

What's up with $\bar{S}$?

We know $|\psi\rangle$ must be supported only on S.

Having now proved A_0, A_1 preserve S, we can wlog assume $\mathcal{H}_A = S$.

Why? $\bar{S}$ is the space of strategies when she isn't going to win with optimal probability.

Thm (on pset 2) For observables $\mathcal{O}_0, \mathcal{O}_1 \in \mathcal{L}(S)$,

For $\mathcal{O}_0^2 = \mathcal{O}_1^2 = \mathbb{1}$ and $\mathcal{O}_0 \mathcal{O}_1 = -\mathcal{O}_1 \mathcal{O}_0$, $\exists$ unitary

$\mathcal{U} : S \to \mathbb{C}^2 \otimes S'$ s.t. $\mathcal{U}\, \mathcal{O}_0\, \mathcal{U}^\dagger = Z \otimes \mathbb{1}_{S'}$

and $\mathcal{U}\, \mathcal{O}_1\, \mathcal{U}^\dagger = X \otimes \mathbb{1}_{S'}$

We can't apply this theorem to A_0, A_1 but we can apply it to $A_0|_S, A_1|_S$ and to $B_0|_T, B_1|_T$ ← analogs.

So, $\exists\ \mathcal{U} : S \to \mathbb{C}^2 \otimes S'$, $V : T \to \mathbb{C}^2 \otimes T'$.

$$\mathcal{U}(A_0|_S)\mathcal{U}^\dagger = Z \otimes \mathbb{1}_{S'} \qquad V(B_0|_T)V^\dagger = H \otimes \mathbb{1}_{T'}$$

$$\mathcal{U}(A_1|_S)\mathcal{U}^\dagger = X \otimes \mathbb{1}_{S'} \qquad V(B_1|_T)V^\dagger = \tilde{H} \otimes \mathbb{1}_{T}.$$

These uniteries give us that Alice and Bob's strategies within S and T are equivalent to the canonical strategy. But the canonical strategy needs $|\psi\rangle$ to be a 4-eigenvector of $(XZ - ZX) \otimes (H\tilde{H} - \tilde{H}H)$ which is uniquely $|EPR\rangle$. So, for $|\psi\rangle \in S \otimes T$,

$$U \otimes V |\psi\rangle = |EPR\rangle \otimes |junk\rangle_{S'T'}.$$

This let's us prove the following theorem

Thm (CHSH rigidity)

given $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and observables $A_0, A_1 \in \mathcal{L}(\mathcal{H}_A)$, $B_0, B_1 \in \mathcal{L}(\mathcal{H}_B)$, s.t. the strategy wins with $\cos^2 \pi/8$ prob. Then $\exists$ local isometries

$$\mathcal{U}_A : \mathcal{H}_A \to \mathbb{C}^2 \otimes \mathcal{H}_{A'} \quad , \quad \mathcal{V}_B : \mathcal{H}_B \to \mathbb{C}^2 \otimes \mathcal{H}_{B'}$$

such that

$$(\mathcal{U}_A \otimes \mathcal{V}_B) |\psi\rangle_{AB} = |EPR\rangle \otimes |junk\rangle_{A'B'}.$$

and

$$(\mathcal{U}_A \otimes \mathcal{V}_B)(A_0 \otimes \mathbb{1}_B)|\psi\rangle = (Z \otimes \mathbb{1})|EPR\rangle \otimes |junk\rangle$$

$$(\mathcal{U}_A \otimes \mathcal{V}_B)(A_1 \otimes \mathbb{1}_B)|\psi\rangle = (X \otimes \mathbb{1})|EPR\rangle \otimes |junk\rangle$$

$$(\mathcal{U}_A \otimes \mathcal{V}_B)(\mathbb{1} \otimes B_0)|\psi\rangle = (\mathbb{1} \otimes H)|EPR\rangle \otimes |junk\rangle$$

$$(\mathcal{U}_A \otimes \mathcal{V}_B)(\mathbb{1} \otimes B_1)|\psi\rangle = (\mathbb{1} \otimes \tilde{H})|EPR\rangle \otimes |junk\rangle$$

This is the best we can do! We can only completely characterize the actions of Alice and Bob on the subspaces S and T. This is what is being expressed here.

What about mixed strategies ρ_{AB}? We can prove something similar

But first we are going to establish some necessary mathematics.

Thm (Schmidt Decomposition)

Any pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed as

$$\sum_{i=1}^{d} \lambda_i |u_i\rangle |v_i\rangle$$

Schmidt coefficients

where $d \leq \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$, $\lambda_i \geq 0$, $\sum \lambda_i^2 = 1$,

$\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ are orthonormal vectors within $\mathcal{H}_A, \mathcal{H}_B$, respt.

This is a special case of singular value decomposition.

Recall SVD, for any matrix $M: \mathcal{H}_B \to \mathcal{H}_A$, $M = \mathcal{U} \Lambda V$

$$\mathcal{U} = \sum_i |u_i\rangle\langle i| \, , \quad \Lambda = \sum_i \lambda_i |i\rangle\langle i| \, , \quad V = \sum_i |i\rangle\langle v_i| .$$

orthonormal basis of $\mathcal{H}_A$. , $\Lambda \geq 0$, orthonormal basis of $\mathcal{H}_B$.

so $$M = \sum_i \lambda_i |u_i\rangle_A \langle v_i|_B .$$

Pf of Schmidt Decomposition:

Let T be the map $\langle v| \mapsto |v\rangle$ for any $|v\rangle \in \mathcal{H}_B$.

For any vector $|\psi\rangle = \sum_{jk} \psi_{jk} |j\rangle|k\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

Consider $M = \sum_{jk} \psi_{jk} |j\rangle\langle k|$.

$$
\begin{aligned}
\text{Then,} \quad |\psi\rangle &= T \circ M \\
&= T\left(\sum_i \lambda_i |u_i\rangle\langle v_i|\right) \\
&\qquad \text{(by SVD)} \\
&= \sum_i \lambda_i |u_i\rangle\langle v_i| .
\end{aligned}
$$

∎

Schmidt decompositions are very useful.

Given $|\psi\rangle_{AB} = \sum_i \lambda_i |u_i\rangle|v_i\rangle$, it is easy to check

$$\psi_A := \operatorname{tr}_B(|\psi\rangle\langle\psi|) = \sum \lambda_i^2 |u_i\rangle\langle u_i|$$

$$\psi_B := \operatorname{tr}_A(|\psi\rangle\langle\psi|) = \sum \lambda_i^2 |v_i\rangle\langle v_i|$$

Def. (Purification)

given a density matrix $\rho_A \in \mathcal{H}_A$, a purification is any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$ s.t. $\text{tr}_{A'}(|\psi\rangle\langle\psi|) = \rho_A$.

A purification is a pure state whose statistics when acting only on A mirror that of ρ_A.

① A purification always exists when $\mathcal{H}_{A'} \cong \mathcal{H}_A$.

$$\rho = \sum_i p_i |u_i\rangle\langle u_i| \quad \text{then} \quad |\psi\rangle = \sum_i \sqrt{p_i}\, |u_i\rangle_A |u_i\rangle_{A'}$$

is a purification.

(Uhlmann's Thm)

② Let $|\psi\rangle_{AA'}$ and $|\tau\rangle_{AA''}$ be two purifications of ρ. Then

$$\exists\, V: \mathcal{H}_{A'} \to \mathcal{H}_{A''} \text{ s.t. } \mathbb{1}_A \otimes V\, |\psi\rangle = |\tau\rangle$$

(Pf sketch) Consider the Schmidt decompositions of $|\psi\rangle$ and $|\tau\rangle$

$$|\psi\rangle = \sum_i \lambda_i |u_i\rangle |v_i\rangle$$

$$|\tau\rangle = \sum_i \mu_i |w_i\rangle |z_i\rangle$$

The Schmidt coefficients of both are the roots of the eigenvalues of ρ.

So $\lambda_i = \mu_i$.

$|u_i\rangle$ and $|w_i\rangle$ must be eigenvectors of ρ.

If distinct (easy case), then $|u_i\rangle = |w_i\rangle$ up to global phase.

Then it remains only to identify a mapping $|v_i\rangle \mapsto |z_i\rangle$. ▨

Why bother with all of this?

Necessary to observe a powerful quantum phenomenon:

Monogamy of entanglement.

Consider any state ρ_{ABE} in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$,

such that ρ_{AB} is pure: $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$.

Then $\rho_{ABE} = |\psi\rangle\langle\psi|_{AB} \otimes \rho_E$.

Pf. ρ_{ABE} is a mixed state so consider a purification $|\varphi\rangle_{ABEE'}$.

But notice, $|\psi\rangle_{AB} \otimes |0,0\rangle_{EE'}$ is a purification of ρ_{AB}.

Uhlmann's theorem gives us that $\exists\ V \in \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_{E'})$

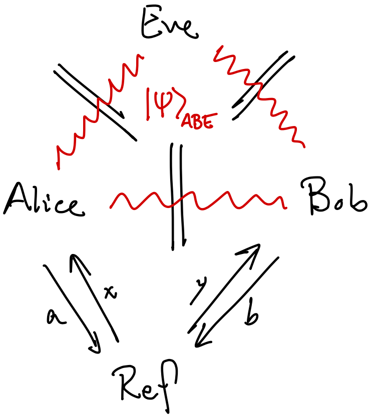
s.t. $|\varphi\rangle_{ABEE'} = |\psi\rangle_{AB} \otimes V|0,0\rangle_{EE'}$

so, A,B are unentangled from E,E'. ⊠

This whole business with E' is tedious. In most cases, we deal with E represents the system of an (Eve)sdropper. We want to typically make arguments where the Eve is as powerful as possible, so we assume Eve has the purification E' as well.

So, we usually assume a pure state $|\psi\rangle_{ABE}$.

Let's consider the CHSH game but this time assume ∃ Eve who may be entangled.



We won't show it, but our proof can be generalized to the following theorem:

Thm (CHSH rigidity) given $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ and observables $A_0, A_1 \in \mathcal{L}(\mathcal{H}_A)$, $B_0, B_1 \in \mathcal{L}(\mathcal{H}_B)$, s.t. the strategy wins with $\cos^2 \pi/8 - \epsilon$ prob. Then $\exists$ local isometries

$$U_A : \mathcal{H}_A \to \mathbb{C}^2 \otimes \mathcal{H}_{A'} \quad , \quad V_B : \mathcal{H}_B \to \mathbb{C}^2 \otimes \mathcal{H}_{B'}$$

such that

$$(U_A \otimes V_B)\, |\psi\rangle_{ABE} \approx_{\sqrt{\epsilon}} |EPR\rangle \otimes |junk\rangle_{A'B'E}$$

and

$$(U_A \otimes V_B)(A_0 \otimes \mathbb{1}_B)\,|\psi\rangle \approx_{\sqrt{\epsilon}} (Z \otimes \mathbb{1})|EPR\rangle \otimes |junk\rangle_{A'B'E}$$

$$(U_A \otimes V_B)(A_1 \otimes \mathbb{1}_B)\,|\psi\rangle \approx_{\sqrt{\epsilon}} (X \otimes \mathbb{1})|EPR\rangle \otimes |junk\rangle_{A'B'E}$$

$$(U_A \otimes V_B)(\mathbb{1} \otimes B_0)\,|\psi\rangle \approx_{\sqrt{\epsilon}} (\mathbb{1} \otimes H)|EPR\rangle \otimes |junk\rangle_{A'B'E}$$

$$(U_A \otimes V_B)(\mathbb{1} \otimes B_1)\,|\psi\rangle \approx_{\sqrt{\epsilon}} (\mathbb{1} \otimes \tilde{H})|EPR\rangle \otimes |junk\rangle_{A'B'E}.$$

where $|u\rangle \approx_{\sqrt{\epsilon}} |v\rangle$ if $\| |u\rangle - |v\rangle \| \leq O(\sqrt{\epsilon})$.

Observations

① This subsumes mixed state strategies for Alice & Bob because that is captured by Eve holding the purification.

② We consider what happens when we win with nearly optimal prob. Then A_0, A_1 approximately anticommute w.r.t. $|\psi\rangle$.

③ Monogamy of entanglement is in play here. Notice that this proves that the identified qubits for Alice & Bob used in the game can only be $O(\sqrt{\epsilon})$ entangled with Eve.

So Alice's measurements of her qubit for an opt $- \epsilon$ strategy will generate a random variable a s.t.

$$H_{min}(a \mid E) \geq 1 - O(\sqrt{\epsilon}).$$

meaning Eve can only guess a with pr $\leq \frac{1}{2} + O(\sqrt{\epsilon})$.

A sketch of how to build certifiable randomness.

Suppose the ref has a small seed of uniform randomness independent from everyone else. He wants more so he buys devices named Alice and Bob from Eve (she built the devices).

He separates Alice and Bob from each other and Eve and uses them to play CHSH knowing that honest Alice produces uniform randomness.

Can he use Alice's outputs as new certified randomness?

Issues:

1. Running CHSH requires 2 bits and only generates 1 bit of randomness.

2. Alice and Bob as devices may keep a

memory of past questions.

We will not handle the second which requires much more advanced techniques.

Meaning, we can assume Alice's action in the t'th round only depends on the t^{th} question asked of her and not her previous questions and answers.

For some $p > 0$,

```
Algorithm   Play CHSH game n total times.
  For $t = 1 \ldots n$,
      With probability $1-p$,   (Generation game)
          ask $x_t = y_t = 0$.
          and record answer $a_t$.
      With probability $p$,   (Test game)
          ask $x_t, y_t$ uniformly randomly.
          check if $a_t \oplus b_t = x_t \cdot y_t$.

  If $\geq 0.849pn$ test games are won, then accept the stored
  $\{a_t\}$ as randomness. Otherwise abort.
```

Since most questions are (0,0), why cant Alice and Bob cheat?

They will then fail the test games.

So, they have to play near optimally in order to not abort.

Analysis

Let μ be the prob of winning standard CHSH by these players.

Then passing the test certifies by Chernoff,

$$X_t = [t \text{ is test round}] \wedge [\text{CHSH passes in round } t] \qquad X = \sum X_t$$

$$\mathbb{E}X = \mu p n$$

$$\Pr\left[\mu \leq \overset{\cos^2 \pi/8}{\omega^*} - \frac{1}{100} \;\middle|\; \text{not abort} \right]$$

$$= \Pr\left[\mu p n \leq \left(\omega^* - \frac{1}{100}\right) n \;\middle|\; X \geq \left(\omega^* - \frac{1}{200}\right) p n \right]$$

$$= \Pr\left[X - \mu p n \geq \frac{pn}{200} \;\middle|\; \text{not abort} \right]$$

$$= \Pr\left[X \geq \mu p n \left(1 + \frac{1}{200\mu}\right) \right] \leq \exp\left(\frac{-\mu p n}{40000\,\mu^2} \right)$$

$$\leq \exp\left(\frac{-pn}{40000\,\mu} \right).$$

μ will end up being a constant $\geq \frac{1}{2}$ so (back of envelope)

$$\Rightarrow \Pr\left[\mu \geq \omega^* - \frac{1}{100} \,\middle|\, \text{not aborting} \right] \geq 1 - 2^{-\Omega(pn)}.$$

By rigidity theorem, then Alice and Bob's strategy is $2\sqrt{\epsilon}$ close to ideal where $\epsilon = \frac{1}{100}$, so Alice's outputs have

$$H_{min}(a_t | E) \geq 4/5.$$

Let δ be the prob. of false certification. Then pick p s.t. $\Omega(pn) = \log \frac{1}{\delta}$.

Algorithm uses $O(pn \log(\frac{1}{p}))$ randomness.

$$= O\left(\log \frac{1}{\delta} \log \frac{n}{\log \frac{1}{\delta}}\right) \leq O\left(\log n \log \frac{1}{\delta}\right).$$

Roughly speaking an exponential increase in randomness.

See Vazirani & Vidick 2012 for full proof with full power adversaries.