Lecture 5

Oct 10, 2024

Answer: YES!

But to prove it, we will need a way to characterize all quantum strategies Alice & Bob could apply.

General quantum strategy of Alice

Input: ρ_{AB} ← some state over Alice and Bob.
Could include ancillas.

Her algorithm:

- Apply unitary U_1 to her qubits.
- Measure qubit 1.
- Apply U_2 to her qubits.
- Measure qubit 1.

⋮

- Apply U_T to her qubits.
- Measure qubit 1 and output value.

Note: this is general enough to include any classical processing of measurements by hw 1 result.

We need to simplify her algorithm.

Step 1: Principle of deferred measurement

Alice's strategy is equivalent to a strategy with only 1 measurement (the final measurement). The new strategy uses T additional ancilla qubits.

Pf.

Recall $\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ or $\mathrm{CNOT}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$.

Let σ_{AB} be the state of the computation before the measument of the 1^{st} qubit. After the measurement the state will be:

$$\sigma_{AB}' = \sum_{k \in \{0,1\}} (|k\rangle\langle k| \otimes \mathbb{1}) \sigma_{AB} (|k\rangle\langle k| \otimes \mathbb{1}).$$

Consider instead initializing an additional ancilla so the state is $\sigma_{AB} \otimes |0\rangle\langle 0|_{Anc}$. Apply CNOT between qubit 1 and ancilla. Then ignore the ancilla for the remainder of the algorithm.

Since the remainder of the alg. ignores the ancilla, we know the measurements are equivalent to that of the state

$$\mathrm{tr}_{anc}\left(CNOT_{1,anc} \left(\sigma_{AB} \otimes |0\rangle\langle 0|_{anc} \right) CNOT_{1,anc} \right)$$

Suffices to show that this equals σ'_{AB}.

Let $\sigma_{AB} = \sum_{i,j \in \{0,1\}} |i\rangle\langle j|_1 \otimes \sigma_{ij}$ ← generic decomp.

$$\left(\sigma_{ij} = (\langle i| \otimes \mathbb{1}) \sigma (|j\rangle \otimes \mathbb{1}) \right) \quad \sigma = \begin{pmatrix} \sigma_{00} & \sigma_{01} \\ \sigma_{10} & \sigma_{11} \end{pmatrix}.$$

$$\mathrm{tr}_{anc}\left(CNOT_{1,anc} \left(\sigma_{AB} \otimes |0\rangle\langle 0|_{anc} \right) CNOT_{1,anc} \right)$$

$$= \mathrm{tr}_{anc}\left(\sum_{i,j \in \{0,1\}} |i,i\rangle\langle j,j|_{1,anc} \otimes \sigma_{ij} \right)$$

$$= \sum_{k \in \{0,1\}} \langle k|_{anc} \otimes \mathbb{1}_{AB} \left(\sum_{i,j \in \{0,1\}} |i,i\rangle\langle j,j|_{1,anc} \otimes \sigma_{ij} \right) |k\rangle_{anc} \otimes \mathbb{1}_{AB}$$

equals 0 unless $k = i$ and $j = k$

$$= \sum_{k \in \{0,1\}} |k\rangle\langle k|_1 \otimes \sigma_{kk}$$

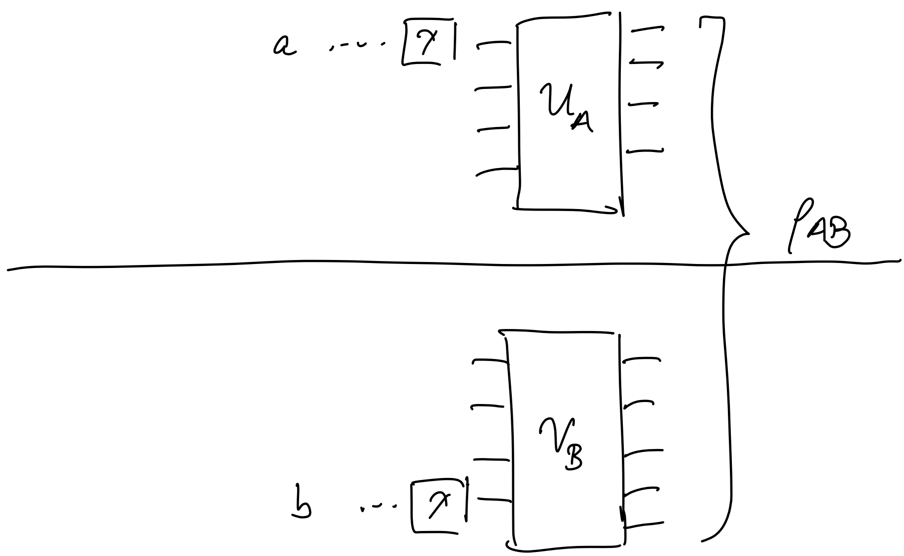
Notice $\sigma' = \sum_{k\in\{0,1\}} (|k\rangle\langle k| \otimes \mathbb{1})\, \sigma_{AB}\, (|k\rangle\langle k| \otimes \mathbb{1})$.

$$= \sum_k |k\rangle\langle k| \otimes \sigma_{kk}.$$

Therefore, entangling with ancilla and "discarding" ancilla is equivalent to measurement.

So, Alice strategy is to apply a unitary U_A and then measure the first qubit, without loss of generality.

Same with Bob.



What is Alice's prob of outputting 1 ?

$$\Pr(\text{outputting } i) = \operatorname{tr}\left(\left(|i\rangle\langle i| \otimes \mathbb{1}\right) U_A \rho_A U_A^\dagger\right)$$

$$= \operatorname{tr}\left(U_A^\dagger \left(|i\rangle\langle i| \otimes \mathbb{1}\right) U_A \rho_A\right)$$

Let $M^i = U_A^\dagger \, |i\rangle\langle i| \otimes \mathbb{1} \, U_A$.

Then $\Pr(\text{outputting } i) = \operatorname{tr}(M_i \rho)$.

Notice $M^0 + M^1 = U_A^\dagger \left(\sum |i\rangle\langle i| \otimes \mathbb{1}\right) U_A$

$$= U_A^\dagger \, \mathbb{1} \, U_A = \mathbb{1}$$

and $M^i \geq 0$, and $(M^i)^2 = M^i$ projector.

This is a special case of a

pos. valued operator valued measurement.

will show up in hw 2.

For now, suffices to observe that Alices strategy can be described by M^0, M^1 proj. for $M^0 + M^1 = \mathbb{1}_A$.

In general, for the CHSH game, Alice's action depends on input x, so her strategy can be expressed by pairs

$\{A_x^0, A_x^1\}_{x \in \{0,1\}}$ s.t. A_x^a proj. and $A_x^0 + A_x^1 = \mathbb{1}_A$.

Same with Bob: $\{B_y^0, B_y^1\}$

Today:

Complete analysis of CHSH game.

Recall we defined the game as Alice and Bob recieve

$x, y \in \{0,1\}$ and answer with $a, b \in \{0,1\}$.

Win condition: $a \oplus b = x \cdot y$.

Switch to $\{a, b\} \in \{-1, +1\}$ and

win condition: $a \cdot b = (-1)^{x \cdot y}$.

So last time we showed that a general strategy for Alice and Bob can be mathematically expressed as

$\{A_x^{(1)}, A_x^{(-1)}\}_{x \in \{0,1\}}$ s.t. $A_x^{(a)}$ proj. and $A_x^{(1)} + A_x^{(-1)} = \mathbb{1}_A$.

Same with Bob: $\{B_y^{(1)}, B_y^{(-1)}\}$

Assume Alice and Bob share a state ρ_{AB}.

Then $\Pr[a, b \mid x, y] = tr\left(A_x^{(a)} \otimes B_y^{(b)} \rho_{AB}\right)$.

$$\Pr[\text{win}] = \sum_{x,y} \Pr[x,y] \cdot \sum_{a,b} \Pr[a,b \mid x,y] \cdot \mathbb{1}\{a \cdot b = (-1)^{xy}\}$$

$$= \frac{1}{4} \sum_{a,b,x,y}' \mathbb{1}\{a \cdot b = (-1)^{xy}\} \operatorname{tr}\left(A_x^{(a)} \otimes B_y^{(b)} \rho_{AB}\right)$$

$$= \frac{1}{4} \sum_{a,b,x,y} \left(\frac{1}{2} + \frac{a \cdot b \cdot (-1)^{xy}}{2}\right) \operatorname{tr}\left(A_x^{(a)} \otimes B_y^{(b)} \rho_{AB}\right)$$

$$= \frac{1}{2} + \frac{1}{8} \sum_{a,b,x,y} ab(-1)^{xy} \operatorname{tr}\left(A_x^{(a)} \otimes B_y^{(b)} \rho_{AB}\right)$$

$$(*) \quad = \frac{1}{2} + \frac{1}{8} \operatorname{tr}\left(\left(\sum_{a,b,x,y} (-1)^{xy} \left(a A_x^{(a)} \otimes b B_y^{(b)}\right)\right) \rho_{AB}\right).$$

To simplify, lets define $A_x := A_x^{(1)} - A_x^{(-1)}$.

Since $A_x^{(1)} + A_x^{(-1)} = \mathbb{1}_A$ and $A_x^{(a)}$ are projectors,

$$A_x = \mathbb{1}_A - 2A_x^{(1)} \quad \text{and}$$

$$A_x^2 = \mathbb{1}_A + 4A_x^{(1)\,2} - 4A_x^{(1)} = \mathbb{1}_A \quad \text{since } A_x^{(1)} \text{ proj.}$$

so A_x^2 has eigenvalues $(-1, 1)$.

Such matrices are called "<u>binary</u> <u>observables</u>".

Notice $\mathbb{E}(a) = \operatorname{tr}(A_x \rho_A)$.

Back to solving $(*)$. Notice that

$$A_x \otimes B_y = \Big(\sum_a a A_x^{(a)}\Big) \otimes \Big(\sum_b b B_y^{(b)}\Big)$$

$$= \sum_{a,b} a A_x^{(a)} \otimes b B_y^{(b)}.$$

So $(*) = \frac{1}{2} + \frac{1}{8} \operatorname{tr}\Big(\underbrace{\Big(\sum_{x,y} (-1)^{xy} A_x \otimes B_y\Big)}_{:= CHSH} \rho_{AB} \Big)$

CHSH is an operator $\in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$. So

Claim: $\operatorname{tr}(CHSH\ \rho_{AB}) \leq \underbrace{\|CHSH\|_{op}}_{\text{max singular value}}$.

Pf. $\rho_{AB} = \sum p_i |\psi_i\rangle\langle\psi_i|$.

unit norm

Then $\operatorname{tr}(CHSH\ \rho_{AB}) = \sum_i p_i \langle\psi_i| CHSH |\psi_i\rangle$

$$\leq \sum_i p_i \|CHSH\| = \|CHSH\|. \quad \square$$

So, $\Pr[\text{win}] \leq \frac{1}{2} + \frac{1}{8} \|CHSH\|$.

Note: $\cos^2 \pi/8 = \frac{1}{2} + \frac{2\sqrt{2}}{8}$.

So suffices to prove, $\|CHSH\| \leq 2\sqrt{2}$, or $\|CHSH^2\| \leq 8$.

Pf.

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

$$= (A_0 + A_1) \otimes B_0 + (A_0 - A_1) \otimes B_1,$$

Use $A_0^2 = A_1^2 = B_0^2 = B_1^2 = \mathbb{1}$ to get

$$CHSH^2 = (A_0 + A_1)^2 \otimes \mathbb{1} + (A_0 - A_1)^2 \otimes \mathbb{1}$$

(no commutation!)

$$+ (A_0 + A_1)(A_0 - A_1) \otimes B_0 B_1$$

$$+ (A_0 - A_1)(A_0 + A_1) \otimes B_1 B_0.$$

$$= 4\mathbb{1} + \underbrace{(A_0 A_1 + A_1 A_0 - A_0 A_1 - A_1 A_0)}_{0} \otimes \mathbb{1}$$

$$+ (A_0 A_1 - A_1 A_0) \otimes (-B_0 B_1)$$

$$+ (A_0 A_1 - A_1 A_0) \otimes (B_1 B_0)$$

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

where $[A_0, A_1]$ = commutator $:= A_0A_1 - A_1A_0$.

Now $\|[A_0,A_1]\| \le \|A_0A_1\| + \|A_1A_0\|$

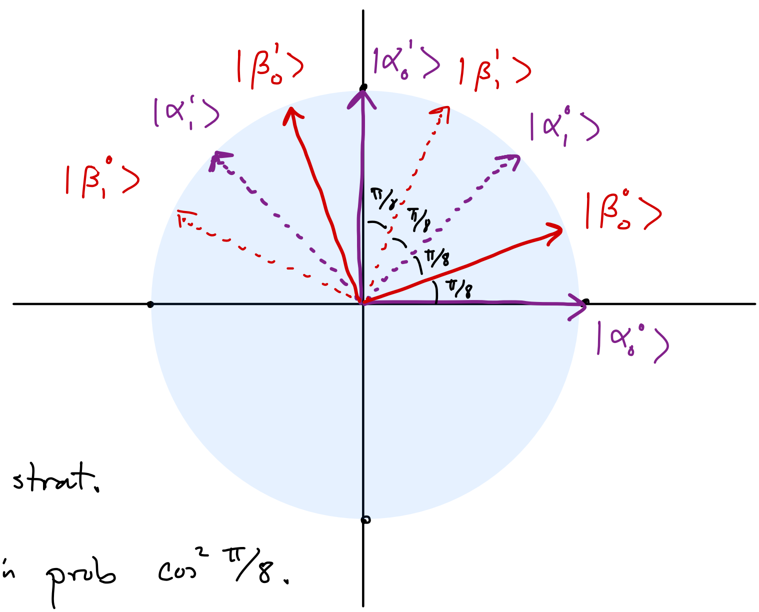
$$\le \|A_0\|\cdot\|A_1\| + \|A_1\|\cdot\|A_0\| = 2.$$

So $\|CHSH\|^2 = 4 + \|[A_0,A_1]\|\cdot\|[B_0,B_1]\|$

$$\le 4 + 2\cdot 2 = 8. \qquad \blacksquare$$

What have we solved?

We proved, the following strategy wins with prob. $\cos^2 \pi/8$.



And that every q. strat. is bounded by win prob $\cos^2 \pi/8$.

Def. (Value of game) For game G,

$\omega(G)$ = max prob winning over classical strat

$\omega^*(G)$ = sup prob. winning over q. strat.

$\omega^*(CHSH) = \cos^2 \pi/8$ and $\omega(CHSH) = 3/4$.

What was the opt strategy, we found?

$A_0^* = |\alpha_0^0\rangle\langle\alpha_0^0| - |\alpha_0^1\rangle\langle\alpha_0^1| = Z$ (phase-flip)

$A_1^* = X$ (bit-flip)

$B_0^* = H$ (Hadamard)

$B_1^* = \tilde{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ ("rotated" Hadamard)

Lets notice that $A_0^* A_1^* = -A_1^* A_0^*$ and $B_0^* B_1^* = -B_1^* B_0^*$.

(anti-commutation).

Furthermore, $|EPR\rangle$ is the unique $2\sqrt{2}$ eigenvector of

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

(easy to computer verify).

Are there any other optimal strategies?

Thm All optimal strategies are unitarily equivalent to to the strategy $(A_0^*, A_1^*, B_0^*, B_1^*, |EPR\rangle)$ given.

we will formally define unitarily equivalent.

Pf. If a strategy is optimal, then all ineq. must be tight:

$$\mathrm{tr}(CHSH\ \rho_{AB}) = 2\sqrt{2} \quad \text{and} \quad \|CHSH\| = 2\sqrt{2}.$$

so $\rho_{AB} = \sum p_i |\psi_i\rangle\langle\psi_i|$ with $\langle\psi_i|CHSH|\psi_i\rangle = 2\sqrt{2}$.

So, ρ_{AB} is a linear combination of "pure strategies";

each of which is a $2\sqrt{2}$ eigenvalued eigenvector of CHSH.

Note: $\|CHSH\| = 2\sqrt{2} \iff \|[A_0, A_1]\| = 2$ and

$$\|[B_0, B_1]\| = 2.$$

$\|[A_0, A_1]\| = 2 \iff A_0$ and A_1 anti-commute.

Thm (on pset 2)

For $A_0^2 = A_1^2 = \mathbb{1}_A$ and $A_0 A_1 = -A_1 A_0$, $\exists$ unitary $\mathcal{U}_A$

s.t. $\mathcal{U}_A A_0 \mathcal{U}_A^\dagger = A_0^* \otimes \mathbb{1} = Z \otimes \mathbb{1}_{A'}$,

and $\mathcal{U}_A A_1 \mathcal{U}_A^\dagger = A_1^* \otimes \mathbb{1} = X \otimes \mathbb{1}_{A'}$.

Likewise $\exists$ V_B s.t. $V_B B_0 V_B^\dagger = B_0^* \otimes \mathbb{1}_{B'}$,

and $V_B B_1 V_B^\dagger = B_1^* \otimes \mathbb{1}_{B'}$.

Therefore,

$$(\mathcal{U}_A \otimes V_B)\, \mathrm{CHSH}\, (\mathcal{U}_A^\dagger \otimes V_B^\dagger) = \mathrm{CHSH}^*_{A_1 B_1} \otimes \mathbb{1}_{A'B'}$$

The only eigenvectors of $\mathrm{CHSH}^* \otimes \mathbb{1}$ of eigenvalue $2\sqrt{2}$

are $|EPR\rangle_{A_1B_1} \otimes |junk\rangle_{A'B'}$.

So, $|\psi\rangle = (\mathcal{U}_A^\dagger \otimes V_B^\dagger)\, |EPR\rangle_{A_1B_1} \otimes |junk\rangle_{A'B'}$.

Putting it all together,

Thm (CHSH Rigidity)

Suppose Alice and Bob win the CHSH game with pr $\cos^2 \pi/8$ with strategy defined by binary observables A_0, A_1, B_0, B_1 and shared quantum state ρ_{AB}.

Then, $\exists$ unitaries U_A and V_B acting on respective systems s.t.

$$(U_A \otimes V_B)\, \rho_{AB}\, (U_A \otimes V_B)^\dagger = |EPR\rangle\langle EPR| \otimes \rho^{junk}_{A'B'}.$$

and

$$U_A A_i U_A^\dagger = A_i^* \otimes \mathbb{1} \text{ with } A_0^* = Z,\ A_1^* = X$$

$$V_B B_i V_B^\dagger = B_i^* \otimes \mathbb{1} \text{ with } B_0^* = H,\ B_1^* = \tilde{H}.$$

Interpretation:

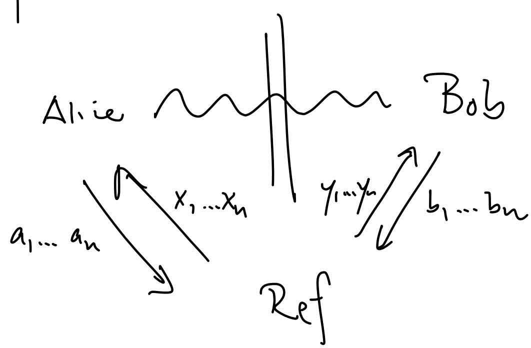
We have no idea what Alice is doing when she recieves x. Her computer could be 10 qubits, 100 qubits, n qubits ...

She could be mining bitcoin with half her device and though could be interacting with the CHSH game.

Nevertheless, by this theorem, we can identify 1 qubit in her device and it must be entangled in an EPR pair with the 1 qubit we know of Bob's.

A way of certifying that Alice & Bob share 1 qubit of entanglement!

Parallel repetition: What if Alice & Bob play n rounds of CHSH in parallel?



If the win with pr $\left[\cos^2(\pi/8)\right]^n$, they share n EPR pairs.

Problem is how to certify that they win with prob exactly $\left[\cos^2 \pi/8\right]^n$.

This is the problem of robustness.

Thm (Robust CHSH rigidity)

Suppose Alice and Bob win the CHSH game with pr $\cos^2 \pi/8 - \epsilon$ with strategy defined by binary observables A_0, A_1, B_0, B_1 and shared quantum state ρ_{AB}.

Then, $\exists$ unitaries U_A and V_B acting on respective systems s.t.

$$(U_A \otimes V_B)\, \rho_{AB}\, (U_A \otimes V_B)^\dagger \approx_{O(\sqrt{\epsilon})} |EPR\rangle\langle EPR| \otimes \rho^{\text{junk}}_{A'B'}.$$

and

$$U_A A_i U_A^\dagger \approx_{O(\sqrt{\epsilon})} A_i^* \otimes \mathbb{1} \text{ with } A_0^* = Z,\ A_1^* = X$$

$$V_B B_i V_B^\dagger \approx_{O(\sqrt{\epsilon})} B_i^* \otimes \mathbb{1} \text{ with } B_0^* = H,\ B_1^* = \tilde{H}.$$

where $\approx_{O(\sqrt{\epsilon})}$ means that the values are $O(\sqrt{\epsilon})$ close in operator norm.

Pf (sketch) $\|CHSH\| \geq 2\sqrt{2} - \epsilon$

$$\Rightarrow \quad \| [A_0, A_1] \otimes [B_0, B_1] \| \geq 4 - 2\epsilon$$

so $\|[A_0, A_1]\| \geq 2 - \epsilon$

Applying HW thm with this ineq. instead gives $O(\sqrt{\epsilon})$-close to optimal solutions.