Are there any other optimal strategies?

Thm All optimal strategies are "equivalent" to the given strategy.

Pf. If a strategy is optimal, then every inequality in pf of optimal value must be tight. So:

$\|CHSH\|_{op} = 2\sqrt{2}$ and $tr(CHSH\, \rho_{AB}) = 2\sqrt{2}$ so

ρ_{AB} is a prob. mixture of pure strategies $|\psi_i\rangle$ s.t.

① $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ ② $\forall\, i,\ \langle\psi_i|CHSH|\psi_i\rangle = 2\sqrt{2}$.

ignore writing $\mathbb{1}_B$ or $\mathbb{1}_A$

$\|CHSH|\psi_i\rangle\| = 2\sqrt{2} \Rightarrow \|[A_0, A_1]|\psi_i\rangle\| = 2$

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

Claim $A_0 A_1 |\psi_i\rangle = -A_1 A_0 |\psi_i\rangle$ but $A_0 A_1$ does not have to equal $-A_1 A_0$ everywhere.

Ex. $A = \begin{pmatrix} Z & \\ & \mathbb{1} \end{pmatrix}$, $A' = \begin{pmatrix} X & \\ & \mathbb{1} \end{pmatrix}$

then A, A' anticommute on vecs $\begin{pmatrix} \alpha \\ \beta \\ 0 \end{pmatrix}$ but not everywhere.

This is the "best" claim we can hope for. We will use CHSH to characterize Alice's computer. However, we can only characterize the part of her computer that plays the game. How it behaves elsewhere we don't know.

Pf of claim Since $\|A_0\|, \|A_1\| \leq 1$, for

$$\underbrace{\|A_0 A_1 |\psi\rangle\|}_{\text{len} \leq 1} + \underbrace{\|-A_1 A_0 |\psi\rangle\|}_{\text{len} \leq 1} \geq \|[A_0, A_1]|\psi\rangle\| = 2$$

only possible if both vectors are the same. □

$\Rightarrow$ define $\{A_0, A_1\} := A_0 A_1 + A_1 A_0$

then, $\{A_0, A_1\} \otimes \mathbb{1}_B |\psi\rangle = 0$.

Let $S \leq \mathcal{H}_A$ be the nullspace of $\{A_0, A_1\}$.

Notice, $|\tau\rangle \in S \implies A_0|\tau\rangle,\ A_1|\tau\rangle \in S$.

Pf. $(A_0A_1 + A_1A_0)\,A_0|\tau\rangle = A_0A_1A_0|\tau\rangle + A_1|\tau\rangle$

$= -A_0A_0A_1|\tau\rangle + A_1|\tau\rangle$

$= -A_1|\tau\rangle + A_1|\tau\rangle$

$= 0.$

So $A_0|\tau\rangle \in S$. Similar pf for $A_1|\tau\rangle$. □

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

A_0, A_1 are block-diagonal w.r.t. decomposition.

$$A_0 = \begin{bmatrix} A_0|_S & 0 \\ 0 & A_0|_{\bar{S}} \end{bmatrix} \qquad A_1 = \begin{bmatrix} A_1|_S & 0 \\ 0 & A_1|_{\bar{S}} \end{bmatrix}$$

And, $A_0|_S$ and $A_1|_S$ must anticommute.

Similarly, $\mathcal{H}_B = T \oplus \overline{T}$ with $T = \ker\{B_0, B_1\}$.

Claim ρ_{AB} is supported only on $S \otimes T \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$.

The remainder of $\mathcal{H}_A$ and $\mathcal{H}_B$ are states that we know the system is not in.

Thm (on Pset 4) For $\Theta_0, \Theta_1 \in \mathcal{X}(S)$, with

① $\Theta_0^2 = \Theta_1^2 = \mathbb{1}$, ② $\Theta_0\Theta_1 = -\Theta_1\Theta_0$, then $\exists$ unitary U s.t.

$U : S \to \mathbb{C}^2 \otimes S'$ with

① $U\Theta_0 U^\dagger = Z \otimes \mathbb{1}_{S'}$

② $U\Theta_1 U^\dagger = X \otimes \mathbb{1}_S$

We can't apply this theorem directly to A_0, A_1 since they don't anticommute.

But $A_0|_S, A_1|_S$ do anticommute. So do $B_0|_T, B_1|_T$.

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

$$U(A_0|_S)U^\dagger = Z \otimes \mathbb{1}_{S'} \qquad V(B_0|_S)V^\dagger = H \otimes \mathbb{1}_{T'}$$
$$U(A_1|_S)U^\dagger = X \otimes \mathbb{1}_{T'} \qquad V(B_1|_S)V^\dagger = \tilde{H} \otimes \mathbb{1}_{T'}.$$

We can extend these unitaries to all $\mathcal{H}_A, \mathcal{H}_B$ by defining them as $\mathbb{1}$ on $\bar{S}$ and $\bar{T}$.

Since $\mathrm{tr}(CHSH\ \rho_{AB}) = 2\sqrt{2} \Rightarrow$

$$4 = \mathrm{tr}\left(\left[A_0|_S, A_1|_S\right] \otimes \left[B_0|_S, B_1|_S\right] \rho_{AB} \right)$$

$$4 = \mathrm{tr}\Big((U \otimes V)\left[A_0|_S, A_1|_S\right] \otimes \left[B_0|_S, B_1|_S\right] (U \otimes V)^\dagger \cdot (U \otimes V)\, \rho_{AB} (U \otimes V)^\dagger \Big)$$

$$= \mathrm{tr}\Big(\left([Z, X] \otimes \mathbb{1}_{S'} \otimes [H, \tilde{H}] \otimes \mathbb{1}_{T'}\right) (U \otimes V)\, \rho_{AB} (U \otimes V') \Big)$$

$$\Rightarrow (U \otimes V)\, \rho_{AB}\, (U \otimes V') = |EPR\rangle\langle EPR| \otimes \rho'_{S'T'}.$$

in order for the eigenvalue to equal 4 as

$|EPR\rangle$ is the unique 4-eigenvector of $[Z, X] \otimes [H, \tilde{H}]$.

This gives the following theorem:

Thm (CHSH rigidity)

If $(\{A_x\}, \{B_y\}, \rho_{AB})$ is a strategy winning with pr $\cos^2 \pi/8$. Then, $\exists$ local isometries,

$U_A : \mathcal{H}_A \to \mathbb{C}^2_{Q_1} \otimes \mathcal{H}'_A$, $V_B : \mathcal{H}_B \to \mathbb{C}^2_{Q_2} \otimes \mathcal{H}'_B$ s.t.

$$(U_A \otimes V_B)\, \rho_{AB}\, (U_A \otimes V_B)^\dagger = |EPR\rangle\langle EPR|_{Q_1Q_2} \otimes \text{junk}_{A'B'}$$

and

$$(U_A \otimes V_B)(A_{0_A} \otimes \mathbb{1}_B)(U_A \otimes V_B)^\dagger = (Z \otimes \mathbb{1}) |EPR\rangle\langle EPR| \otimes junk_{A'B'}.$$

$$(U_A \otimes V_B)(A_{1_A} \otimes \mathbb{1}_B)(U_A \otimes V_B)^\dagger = (X \otimes \mathbb{1}) |EPR\rangle\langle EPR| \otimes junk_{A'B'}.$$

$$(U_A \otimes V_B)(\mathbb{1}_A \otimes B_{0_B})(U_A \otimes V_B)^\dagger = (\mathbb{1} \otimes H) |EPR\rangle\langle EPR| \otimes junk_{A'B'}.$$

$$(U_A \otimes V_B)(\mathbb{1}_A \otimes B_{1_B})(U_A \otimes V_B)^\dagger = (\mathbb{1} \otimes \tilde{H}) |EPR\rangle\langle EPR| \otimes junk_{A'B'}.$$

Rigidity

Consider starting with a density matrix ρ_{ABE}

and a strategy $(\{A_x\}, \{B_y\}, \rho_{ABE})$ that wins w prob

$$\cos^2 \pi/8 - \epsilon$$

Then every equation in the previous thm is replaced by $\approx_{O(\sqrt{\epsilon})}$

where $\sigma \approx_\delta \rho$ if $\|\sigma - \rho\|_1 \leq \delta$.

And $junk_{A'B'}$ is replaced with $junk_{A'B'E}$.

Proof (sketch)

Follow the proof of this theorem. We will show that the strategy state must be all but $O(\sqrt{\epsilon})$ supported on anticommuting subspace. From here we extract out approximate strategies.

Implications

① Even with only near perfect strategies, Alice & Bob share an EPR pair and measure it for identifying answers.

② The honest state is $O(\sqrt{\epsilon})$ close to unentangled (at least the parts of Alice & Bob that are being used to play the game)

and unentangled with <u>any</u> Eve!

③ Alice's honest measurements are $O(\sqrt{\epsilon})$ close to Z- and X- on an EPR pair.

Generating randomness: Alice's output a satisfies

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

For this class, it suffices to interpret this as Eve can only guess a with $pr \leq 1/2 + O(\sqrt{\epsilon})$.

A sketch on 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 we use Alice's outputs as new certified randomness?

Issues:

① Running CHSH requires the Ref to spend 2 bits of randomness and generates < 1 bit of randomness.

② The Alice & Bob devices can keep a memory.

↑ This is hard to handle. Instead we will assume that the devices are identical in between rounds, or equivalently that the shared state is $\rho_{AB,E_i}^{\otimes n}$.

Randomness Generation Algorithm

Fix $\eta > 0$ small constant and $0 \leq p \leq 1/2$ and integer n.

At high level, we will ask Alice & Bob to play CHSH n times.

For $t = 1, \ldots, n$:

with probability $1 - p$ (generation game)

ask questions $x_t = y_t = 0$ and record answer a_t.

with probability p (test game)

sample x_t, y_t uniformly and check if $a_t \oplus b_t = x_t y_t$.

If $\left(\cos^2 \pi/8 - \eta\right) n$ test games are won, then accept stored $\{a_t\}$ as a source of randomness. Otherwise reject.

Since most questions are $(0,0)$, why can't Alice & Bob cheat?
They will fail the test games.

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