Protocol

Alice $|+\rangle_x$ ← Choice for x

$|+\rangle_r$ ← Choice for r

$\frac{1}{2}\mathbb{1}_H$ ← Alice's part of $|GHZ\rangle$

$|0\rangle_s$ ← message to Bob

$|0\rangle_A$ ← Alice's GHZ outcome, to be determined

ρ_0 = Alice's state after measuring to get a $+$ creating S.

$Tr_S(\rho_0)$ = Alice's state after sending S to Bob.

Bob now has a purification of $Tr_S(\rho_0)$, so purifying the post-measured state, and S.

$\rho_1 = \rho_0 + G$ space. So $Tr_G(\rho_1) = Tr_S(\rho_0)$

First check: Alice measures ρ_1 to see if $x \oplus y = 1$.

$$\max \langle \Pi_{11}, \rho_1 \rangle$$
$$Tr_G(\rho_1) = Tr_S(\rho_0)$$

This should give 0.75 (or less, perhaps).

Full protocol SDP

Alice appends $\frac{1}{2}\mathbb{I}_Y$ to ρ_1 So Bob has a copy/ a purification.

Bob responds w/ d (in space D) $d = b \oplus c$ here.

Alice checks if $a \oplus d = xy(x \oplus y \oplus 1) \oplus 1$

SDP: $\max \langle \Pi_2, \rho_2 \rangle$ ← checks if $x \oplus y = 1$ and $a \oplus d = \ldots$

$$\mathrm{Tr}_D(\rho_2) = \rho_1 \otimes \tfrac{1}{2}\mathbb{I}_Y$$

$$\mathrm{Tr}_G(\rho_1) = \mathrm{Tr}_S(\rho_0)$$

$\rho_0 \in \mathrm{Pos}(HXRAS)$

$\rho_1 \in \mathrm{Pos}(HXRAG)$

$\rho_2 \in \mathrm{Pos}(HXRAGYD)$

$$\sigma_0 = \tfrac{1}{2}\mathbb{I}_H \otimes |+\rangle\langle+|_X \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_S$$

$$\sigma_1 = U\left(\tfrac{1}{2}\mathbb{I}_N \otimes |+\rangle\langle+|_X \otimes |+\rangle\langle+|_R \otimes |0\rangle\langle 0|_A\right)U^\dagger \otimes |0\rangle\langle 0|_S$$

$U = I_{GHZ}$

$\sigma_2 =$ creates S from a, x, r.

↑ This is ρ_0, broken up into steps.

Continuity argument

Totally made-up lemma

Keep doing GHZ n times.

Then $\|\rho - \rho_{actual}\| \leq f(n)$

- ρ: as defined above
- ρ_{actual}: approximation
- $f(n)$: goes to 0 as $n \to \infty$

Lemma

α = SDP value from above.

α_{actual} = SDP value using ρ_{actual} instead of ρ.

$|\alpha - \alpha_{actual}| \to 0$ as $n \to \infty$.

Proof: ① Take the dual

② SDP magic.

③ Profit.

□

Concern: Since in this particular protocol implementation, Bob does not separate the "b & c boxes" there is not really much "GHZ" happening. I can't remember if this should be an issue or not. (In any case, 3/4 is an upper bound.)

Question: If Bob sends back boxes B & C to Alice, do we get a nice SDP still? We might need NPA at that point.