CS/Ph120 Homework 4 Solutions

November 3, 2016

Problem 1: Robustness of GHZ and W states, part 2

Solution: (Due to Bolton Bailey)

(a)
For the GHZ state, we have

$$Tr_N|GHZ_N\rangle\langle GHZ_N| = \frac{1}{2}\left(|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1} + |1\rangle^{\otimes N-1}\langle 1|^{\otimes N-1}\right)$$

So therefore, the rank is $r_{GHZ} = 2$.
For the W state, we have

$$|W_N\rangle = \sqrt{\frac{N-1}{N}}|W_{N-1}\rangle \otimes |0\rangle + \frac{1}{\sqrt{N}}|0\rangle^{\otimes N-1} \otimes |1\rangle$$

So we get

$$Tr_N|W_N\rangle\langle W_N| = \frac{N-1}{N}|W_{N-1}\rangle\langle W_{N-1}| + \frac{1}{N}|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1}$$

And so the rank is $r_W = 2$.
(b)
The minimum purity for a density matrix ρ on a d-dimensional vector space is $\frac{1}{d}$. To see that this can be attained, consider

$$\rho = \frac{1}{d}\mathbb{I}_d$$

This matrix is positive semidefinite as a postive multiple of the identiy, and it has trace 1, since the $\mathbb{I}_d$ has trace d. Note that

$$\rho^2 = \frac{1}{d^2}\mathbb{I}_d^2 = \frac{1}{d^2}\mathbb{I}_d$$

And so

$$Tr\rho^2 = \frac{1}{d^2}d = \frac{1}{d}$$

To see it is impossible to have a density matrix of this dimension with a smaller purity, note that

$$Tr\rho^2 = \sum_{1 \leq i \leq d} \langle i|\rho^2|i\rangle$$

To see it is impossible to have a density matrix of this dimension with a smaller purity, let

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

And so therefore

$$\rho^2 = \sum_{i,j} p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|$$

$$Tr\rho^2 = Tr\left(\sum_{i,j} p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|\right)$$

By linearity of the trace

$$Tr\rho^2 = \sum_{i,j} p_i p_j Tr(|\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|)$$

By invariance of trace under cyclic permutations

$$Tr\rho^2 = \sum_{i,j} p_i p_j Tr(\langle\psi_j|\psi_i\rangle\langle\psi_i|\psi_j\rangle)$$

$$Tr\rho^2 = \sum_{i,j} p_i p_j \langle\psi_j|\psi_i\rangle\langle\psi_i|\psi_j\rangle$$

$$Tr\rho^2 = \sum_{i,j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2$$

Now, we separate the sum into the cases where $i = j$ and $i \neq j$

$$Tr\rho^2 = \sum_i p_i^2 |\langle\psi_i|\psi_i\rangle|^2 + \sum_{i \neq j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2$$

Since $\langle\psi_i|\psi_i\rangle = 1$, we get

$$Tr\rho^2 = \sum_i p_i^2 + \sum_{i \neq j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2$$

Now, since the p_i sum to 1, the minimum value of the sum of the p_i^2 is $\frac{1}{d}$ by the Cauchy-Schwarz inequality. The minimum value of $|\langle\psi_i|\psi_j\rangle|^2$ is 0 since the norm squared is nonnegative.

$$Tr\rho^2 \geq \frac{1}{d}$$

As we claimed.

The maximum value of the purity of a density matrix on d dimensions is 1. To see that this can be attained, consider

$$\rho = |0\rangle\langle 0|$$

Which is a pure density matrix, and satisfies

$$Tr\rho^2 = Tr(|0\rangle\langle 0|0\rangle\langle 0|) = Tr(\langle 0|0\rangle\langle 0|0\rangle) = 1$$

To see that this is maximal, recall that we have shown for arbitrary

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

That

$$Tr\rho^2 = \sum_{i,j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2$$

And since $0 \leq |\langle\psi_i|\psi_j\rangle|^2 \leq 1$, and p_i, p_j are positive

$$Tr\rho^2 = \sum_{i,j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2 \leq \sum_{i,j} p_i p_j \leq 1 \cdot 1 = 1$$

So 1 is the maximum purity.

(c)

As a state gets more entangled, we expect the purity to decrease. We think of a state being more entangled as the partial state being more heavily correlated with the other half of the bipartite state. Thus, if we trace out the other state, the partial state will be more mixed.

(d)

Again, we have

$$Tr_N|GHZ_N\rangle\langle GHZ_N| = \frac{1}{2}\left(|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1} + |1\rangle^{\otimes N-1}\langle 1|^{\otimes N-1}\right)$$

And the purity of this state is

$$\begin{aligned} Tr\left((Tr_N|GHZ_N\rangle\langle GHZ_N|)^2\right) &= Tr\left(\frac{1}{4}\left(|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1} + |1\rangle^{\otimes N-1}\langle 1|^{\otimes N-1}\right)^2\right) \\ &= Tr\left(\frac{1}{4}\left(|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1} + |1\rangle^{\otimes N-1}\langle 1|^{\otimes N-1}\right)\right) \\ &= \frac{1}{2} \end{aligned}$$

So in the limit as $N \to \infty$, the purity of this state is $\frac{1}{2}$

(e)

Evaluating the purity

$$\begin{aligned} Tr\left((Tr_N|W_N\rangle\langle W_N|)^2\right) &= Tr\left(\frac{N-1}{N}|W_{N-1}\rangle\langle W_{N-1}| + \frac{1}{N}|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1}\right)^2 \\ &= Tr\left(\left(\frac{N-1}{N}\right)^2 |W_{N-1}\rangle\langle W_{N-1}| + \left(\frac{1}{N}\right)^2 |0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1}\right) \\ &= \left(\frac{N-1}{N}\right)^2 + \left(\frac{1}{N}\right)^2 \\ &= \frac{N^2 - 2N + 2}{N^2} \end{aligned}$$

So in the limit as $N \to \infty$, the purity of this state is 1. Since this value is higher than that for the GHZ states, we can conclude the W states are more robust, as they remain mostly pure even when a bit is traced out.
(f)
We now repeat the analysis tracing out n qubits instead of 1, which we will indicate by Tr_B, Again, we have

$$Tr_B|GHZ_N\rangle\langle GHZ_N| = \frac{1}{2}\left(|0\rangle^{\otimes N-n}\langle 0|^{\otimes N-n} + |1\rangle^{\otimes N-n}\langle 1|^{\otimes N-n}\right)$$

And the purity of this state is

$$\begin{aligned}
Tr\left((Tr_B|GHZ_N\rangle\langle GHZ_N|)^2\right) &= Tr\left(\frac{1}{4}\left(|0\rangle^{\otimes N-n}\langle 0|^{\otimes N-n} + |1\rangle^{\otimes N-n}\langle 1|^{\otimes N-n}\right)^2\right) \\
&= Tr\left(\frac{1}{4}\left(|0\rangle^{\otimes N-n}\langle 0|^{\otimes N-n} + |1\rangle^{\otimes N-n}\langle 1|^{\otimes N-n}\right)\right) \\
&= \frac{1}{2}
\end{aligned}$$

So no matter how many bits are traced out of the GHZ density matrix, the purity is $\frac{1}{2}$ and so in the limit as $N \to \infty$, the purity is $\frac{1}{2}$.
Evaluating the purity for the W density matrix

$$\begin{aligned}
Tr\left((Tr_B|W_N\rangle\langle W_N|)^2\right) &= Tr\left(\frac{N-n}{N}|W_{N-1}\rangle\langle W_{N-1}| + \frac{n}{N}|0\rangle^{\otimes N-n}\langle 0|^{\otimes N-n}\right)^2 \\
&= Tr\left(\left(\frac{N-n}{N}\right)^2|W_{N-n}\rangle\langle W_{N-n}| + \left(\frac{n}{N}\right)^2|0\rangle^{\otimes N-n}\langle 0|^{\otimes N-n}\right) \\
&= \left(\frac{N-n}{N}\right)^2 + \left(\frac{n}{N}\right)^2 \\
&= \frac{N^2 - 2Nn + 2n^2}{N^2}
\end{aligned}$$

So in the limit as $N \to \infty$, the purity of this state still goes to 1 (although slower for larger N). Since this value is higher than that for the GHZ states, we can again conclude the W states are more robust, as they remain mostly pure even when many bits are traced out.

Problem 2: Dimension of a purifying system

Solution: (Due to De Huang)

(a) Let r be the Schmidt rank of $|\Psi\rangle_{AB}$, then $D \geq r$. On the other hand, given

$$\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |3\rangle\langle 3|),$$

we have

$$r = \text{rank}(tr_B|\Psi\rangle\langle\Psi|_{AB}) = \text{rank}(\rho_A) = 2.$$

Therefore $D \geq 2$, the minimum value of D is no less than 2. In particular, if we let B be the space of single qubit($D = 2$), and take

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |3\rangle_A|1\rangle_B),$$

then we have $tr_B|\Psi\rangle\langle\Psi|_{AB} = \rho_A$. Thus the minimum of D is 2.

(b) We can rewrite ρ_A as

$$\rho_A = \frac{1}{5}|1\rangle\rangle\langle 1| + \frac{2}{5}\big((\frac{1}{\sqrt{2}}|2\rangle + \frac{1}{\sqrt{2}}|3\rangle)(\frac{1}{\sqrt{2}}\langle 2| + \frac{1}{\sqrt{2}}\langle 3|)\big) + \frac{2}{5}\big((\frac{1}{\sqrt{2}}|4\rangle + \frac{1}{\sqrt{2}}|5\rangle)(\frac{1}{\sqrt{2}}\langle 4| + \frac{1}{\sqrt{2}}\langle 5|)\big).$$

Notice that $|1\rangle$, $\frac{1}{\sqrt{2}}(|2\rangle + |3\rangle)$, $\frac{1}{\sqrt{2}}(|4\rangle + |5\rangle)$ are orthogonal to each other, we have

$$\text{rank}(\rho_A) = 3.$$

Agian we have

$$D \geq \text{rank}(tr_B|\Psi\rangle\langle\Psi|_{AB}) = \text{rank}(\rho_A) = 3.$$

In particular, if we let B be a 3 dimensional qudit space, and take

$$\Psi\rangle_{AB} = \frac{1}{\sqrt{5}}|1\rangle_A|0\rangle_B + \frac{1}{\sqrt{5}}(|2\rangle + |3\rangle)_A|1\rangle_B + \frac{1}{\sqrt{5}}(|4\rangle + |5\rangle)_A|2\rangle_B,$$

then we have $tr_B|\Psi\rangle\langle\Psi|_{AB} = \rho_A$. Thus the minimum of D is 3.

(c) For a general ρ_A, let r be the rank of ρ_A. Consider the eigenvalue decomposition of ρ_A,

$$\rho_A = \sum_{i=0}^{r-1} \lambda_i |\phi_i\rangle\langle\phi_i|,$$

where $|\phi_i\rangle$, $i = 0, 1, \ldots, r-1$, are normalized orthogonal eigen states, $\lambda_i > 0$, $i = 0, 1, \ldots, r-1$, and $\sum_{i=0}^{r-1} \lambda_i = 1$. If $tr_B|\Psi\rangle\langle\Psi|_{AB} = \rho_A$, then

$$D \geq \text{Schmidt rank}(|\Psi_{AB}\rangle) = \text{rank}(tr_B|\Psi\rangle\langle\Psi|_{AB}) = \text{rank}(\rho_A) = r.$$

In particular, let B be a r dimensional qudit space with standard baisi $\{|i\rangle,\ i = 0, 1, \ldots, r-1\}$, and take

$$|\Psi\rangle_{AB} = \sum_{i=0}^{r-1} \sqrt{\lambda_i}|\phi_i\rangle_A|i\rangle_B,$$

then we have $tr_B|\Psi\rangle\langle\Psi|_{AB} = \rho_A$, and thus the minimum of D is r.

(d) Still, consider the eigenvalue decomposition of ρ_A with rank r,

$$\rho_A = \sum_{i=0}^{r-1} \lambda_i |\phi_i\rangle\langle\phi_i|,$$

where $\{|\phi_i\rangle,\ i=0,1,\dots,d-1\}$ is a orthogonal basis of the qudit space A, $\lambda_i > 0,\ i = 0,1,\dots,r-1$, and $\sum_{i=0}^{r-1}\lambda_i = 1$.

Also consider the eigenvalue decomposition of σ_{AB},

$$\sigma_{AB} = \sum_{k=0}^{r'-1} s_k |\Psi_k\rangle\langle\Psi_k|_{AB},$$

where $r' = \text{rank}(\sigma_{AB})$, and $s_k > 0,\ k = 0,1,\dots,r'-1$.

(i) First we find the lowest attainable rank of σ_{AB}. For each $|\Psi_k\rangle_{AB}$, we have

$$\text{rank}(tr_B(|\Psi_k\rangle\langle\Psi_k|_{AB})) = \text{Schmidt rank}(|\Psi_k\rangle_{AB}) \leq m,$$

since the dimension of B system is m Then we have

$$\text{rank}(tr_B\sigma_{AB}) = \text{rank}\big(\sum_{k=0}^{r'-1} s_k tr_B(|\Psi_k\rangle\langle\Psi_k|_{AB})\big) \leq \sum_{k=0}^{r'-1}\text{rank}\big(tr_B(|\Psi_k\rangle\langle\Psi_k|_{AB})\big) \leq r' \times m.$$

But since $tr_B(\sigma_{AB}) = \rho_A$, we have

$$\text{rank}(tr_B\sigma_{AB}) = \text{rank}(\rho_A) = r,$$

and thus we get

$$r' \times m \geq r, \quad \text{i.e.} \quad r' \geq \lceil \frac{r}{m} \rceil,$$

since r' is an integer. Let $p = \lfloor \frac{r}{m} \rfloor$, $q = r - mp$, then we can take

$$s_k = \sum_{i=0}^{m-1}\lambda_{mk+i}, \quad |\Psi_k\rangle_{AB} = \frac{1}{\sqrt{s_k}}\sum_{i=0}^{m-1}\sqrt{\lambda_{mk+i}}|\phi_{mk+i}\rangle_A|i\rangle_B, \quad k = 1,2,\dots,p-1,$$

$$s_p = \sum_{i=0}^{q-1}\lambda_{mp+i}, \quad |\Psi_p\rangle_{AB} = \frac{1}{\sqrt{s_p}}\sum_{i=0}^{q-1}\sqrt{\lambda_{mp+i}}|\phi_{mp+i}\rangle_A|i\rangle_B, \quad \text{if } q > 0.$$

It's easy to check that $|\Psi_k\rangle,\ k = 0,1,\dots,p$, are orthogonal to each other, and that

$$tr_B(\sigma_{AB}) = \rho_A,$$

$$r' = \text{rank}(\sigma_{AB}) = p + \text{sign}(q)\cdot 1 = p + \lceil \frac{r}{m} \rceil - \lfloor \frac{r}{m} \rfloor = \lceil \frac{r}{m} \rceil.$$

In this case the lower-bound is achieved. Thus the minimum attainable rank of σ_{AB} is $\lceil \frac{r}{m} \rceil$.

(ii) Next we find the highest attainable purity of σ_{AB}, i.e. the maximum of

$$tr(\sigma_{AB}^2) = \sum_{k=0}^{r'-1} s_k^2.$$

We now should find out the constraints on $s = (s_0, s_2, \dots, s_r')$(notice the we now have no upper bound on r', even though there is indeed one as $r' \leq m \times r$). Let Ω be the feasible set for s, and that s^* be an optimal solution that achieves the maximum of attainable purity.

The first constraints on s are

$$s_k \geq 0,\ \ k = 0, 1, \ldots, r',\quad \sum_{k=0}^{r'-1} s_k = 1,$$

since σ_{AB} is a density matrix. Before we go further, we give a Lemma: if $a \geq b \geq 0, c \geq d \geq 0,\ a + b = c + d = e,\ a \geq c$, then $a^2 + b^2 \geq c^2 + d^2$.

Proof:

$$\begin{aligned} a^2 + b^2 - (c^2 + d^2) &= (a - c)(a + c) + (b - d)(b + d) \\ &= (a - c)(a + c) + (c - a)(2e - a - c) \\ &= (a - c)(2a + 2c - 2e) \\ &\geq 0. \end{aligned}$$

Now we inductively definde

$$g_0^* = \max_{s\in\Omega}\ s_0,\quad g_k^* = \max_{s\in\Omega, s_i = g_i^*, i=0,\ldots,k-1} s_k\ ,\quad k = 1, 2, \ldots, r' - 1,$$

then using the lemma, we can always make $s_k^* = g_k^*,\ k = 0, 1, \ldots, r' - 1$(it's not a hard proof, and we skip it here). We should find out what g_k^* are.

Let's assume that in the expression of σ_{AB} we give above,

$$|\Psi_k\rangle_{AB} = \sum_{i=0}^{r-1}\sum_{j=0}^{m-1} \alpha_{i,j}^k |\phi_i\rangle_A |j\rangle_B,$$

where

$$\sum_{i=0}^{r-1}\sum_{j=0}^{m-1} |\alpha_{i,j}^k|^2 = \langle\Psi_k|\Psi_k\rangle = 1,\quad k = 0, 1, \ldots, r' - 1,$$

$$\sum_{i=0}^{r-1}\sum_{j=0}^{m-1} \alpha_{i,j}^k \overline{\alpha_{i,j}^l} = \langle\Psi_l|\Psi_k\rangle = 0,\quad k \neq l,$$

since $|\Psi_k\rangle_{AB}$ are normalized and orthogonal to each other. The condition $tr_B(\sigma_{AB}) = \rho_A$ gives that

$$\lambda_i = \sum_{k=0}^{r'-1} s_k \sum_{j=0}^{m-1} |\alpha_{i,j}^k|^2,\quad i = 0, 1, \ldots, r - 1.$$

Now define matrices $A_k \in \mathbb{C}^{r\times m}$ as

$$(A_k)_{i,j} = \sqrt{s_k} a_{i,j}^k,\quad k = 0, 1, \ldots, r' - 1,$$

then all the constraints above can be summarized as

$$\sum_{k=0}^{r'-1} A_k A_k^\dagger = \Lambda = \begin{pmatrix} \lambda_0 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{r-1} \end{pmatrix},$$

$$tr(A_kA_k^\dagger) = s_k, \quad k = 0, 1, \ldots, r' - 1; \quad tr(A_kA_l^\dagger) = 0, \quad k \neq l.$$

We first give a lemma without proof: if $m \leq r$, then

$$\max_{P_1, P_2 \in \Omega'} tr(P_1^\dagger M P_2) = \sum_{i=1}^{m} \sigma_i(M), \quad \forall M \in \mathbb{C}^{r\times r},$$

where $\Omega' = \{P \in \mathbb{C}^{r\times m} : P^\dagger P = \mathbb{I}_m\}$, and $\sigma_i(M)$ denote the i_{th} large singular value of M.

Assume that $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_r > 0$. Then for our case, the lemma above reduces to

$$\max_{P_1, P_2 \in \Omega'} tr(P_1^\dagger \Lambda P_2) = \sum_{i=0}^{m-1} \lambda_m.$$

Consider the reduced eigenvalue decomposition of $A_0A_0^k$,

$$A_0A_0^k = Q\Sigma Q^\dagger,$$

where $Q \in \Omega'$, and $\Sigma \in \mathbb{C}^{m\times m}$ is a positive diagonal matrix. Then since

$$A_0A_0^k \leq \sum_{k=0}^{r'-1} A_kA_k^\dagger = \Lambda, \quad \Longrightarrow \quad \Sigma = Q^\dagger A_0A_0^k Q \leq Q^\dagger \Lambda Q,$$

we have

$$s_0 = tr(A_0A_0^k) = tr(\Sigma) \leq tr(Q^\dagger \Lambda Q) \leq \max_{P_1, P_2 \in \Omega'} tr(P_1^\dagger \Lambda P_2) = \sum_{i=0}^{m-1} \lambda_m,$$

thus $g_0^* \leq \sum_{i=0}^{m-1} \lambda_m$. Recall that in (d)(i) we provided an example in which $s_0 = \sum_{i=0}^{m-1} \lambda_m$, therefore we indeed have $g_0^* = \sum_{i=0}^{m-1} \lambda_m$.

Let $p = \lfloor \frac{r}{m} \rfloor$, $q = r - mp$. Then similarly we can prove that

$$g_k^* = \sum_{i=0}^{m-1} \lambda_{mk+i}, \ k = 0, 1, \ldots, p - 1,$$

and if $q > 0$, $g_p^* = \sum_{i=0}^{q-1} \lambda_{mp+i}$. Now using the previous result, we can always make

$$s_k^* = g_k^* = \sum_{i=0}^{m-1} \lambda_{mk+i}, \ k = 0, 1, \ldots, p - 1; \quad s_p^* = g_p^* = \sum_{i=0}^{q-1} \lambda_{mp+i}, \text{ if } q > 0,$$

and therefore the highest attainable purity of σ_{AB} is

$$\sum_{k=0}^{p-1} (s_k^*)^2 + \text{sign}(q)(s_p^*)^2 = \sum_{k=0}^{p-1} \Big(\sum_{i=0}^{m-1} \lambda_{mk+i} \Big)^2 + \text{sign}(q) \Big(\sum_{i=0}^{q-1} \lambda_{mp+i} \Big)^2,$$

where $\text{sign}(q) = 1$, if $q > 0$; $\text{sign}(q) = 0$, if $q = 0$. Indeed the example in (d)(i),

$$s_k = \sum_{i=0}^{m-1} \lambda_{mk+i}, \quad |\Psi_k\rangle_{AB} = \frac{1}{\sqrt{s_k}} \sum_{i=0}^{m-1} \sqrt{\lambda_{mk+i}} |\phi_{mk+i}\rangle_A |i\rangle_B, \quad k = 1, 2, \ldots, p - 1,$$

$$s_p = \sum_{i=0}^{q-1} \lambda_{mp+i}, \quad |\Psi_p\rangle_{AB} = \frac{1}{\sqrt{s_p}} \sum_{i=0}^{q-1} \sqrt{\lambda_{mp+i}} |\phi_{mp+i}\rangle_A |i\rangle_B, \quad \text{if } q > 0,$$

achieves this maximum of attainable purity.

Problem 3: Secret sharing among three people

Solution: (Due to Bolton Bailey)

(a) We compute the reduced density matrix ρ_A

$$|\Psi\rangle\langle\Psi| = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C + (-1^b)|1\rangle_A|1\rangle_B|1\rangle_C)\frac{1}{\sqrt{2}}(\langle 0|_A\langle 0|_B\langle 0|t_C + (-1^b)\langle 1|_A\langle 1|_B\langle 1|t_C)$$

$$|\Psi\rangle\langle\Psi| = \frac{1}{2}(|000\rangle\langle 000|_{ABC} + (-1^b)|000\rangle\langle 111|_{ABC} + (-1^b)|111\rangle\langle 000|_{ABC} + |111\rangle\langle 111|_{ABC}+)$$

$$|\Psi\rangle\langle\Psi| = \frac{1}{2}(|0\rangle\langle 0|_A\otimes|00\rangle\langle 00|_{BC}+(-1^b)|0\rangle\langle 1|_A\otimes|00\rangle\langle 11|_{BC}+(-1^b)|1\rangle\langle 0|_A\otimes|11\rangle\langle 00|_{BC}+|1\rangle\langle 1|_A\otimes|11\rangle\langle 11|_B$$

$$Tr_{BC}|\Psi\rangle\langle\Psi| = \frac{1}{2}(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A) = \frac{1}{2}\mathbb{I}$$

So ρ_A is the maximally mixed state, no matter the value of b. Thus, A alone gains no information about the secret. By the symmetry of the state Ψ, we see that the other density matrices are the same

$$Tr_{AC}|\Psi\rangle\langle\Psi| = Tr_{AB}|\Psi\rangle\langle\Psi| = \frac{1}{2}\mathbb{I}$$

$$\rho_A = \rho_B = \rho_C = \frac{1}{2}\mathbb{I}$$

So none of the three can recover the secret on their own.

(b) We compute the two-party reduced density matrix ρ_{BC}, from part (b)

$$|\Psi\rangle\langle\Psi| = \frac{1}{2}(|0\rangle\langle 0|_A\otimes|00\rangle\langle 00|_{BC}+(-1^b)|0\rangle\langle 1|_A\otimes|00\rangle\langle 11|_{BC}+(-1^b)|1\rangle\langle 0|_A\otimes|11\rangle\langle 00|_{BC}+|1\rangle\langle 1|_A\otimes|11\rangle\langle 11|_B$$

So

$$Tr_A|\Psi\rangle\langle\Psi| = \frac{1}{2}(|00\rangle\langle 00|_A + |11\rangle\langle 11|_A)$$

So ρ_{BC} is the same mixed state, no matter the value of b. Thus, B and C together gain no information about the secret. By the symmetry of the state Ψ, we see that the other two-party density matrices are again the same

$$Tr_B|\Psi\rangle\langle\Psi| = Tr_C|\Psi\rangle\langle\Psi| = \frac{1}{2}(|00\rangle\langle 00|_A + |11\rangle\langle 11|_A)$$

So these pairs also do not have any information about the secret.

(c) Consider the following LOCC protocol. Alice, Bob and Charlie all apply local Hadamard transformations to their qubit. This yields the state

$$\begin{aligned}
H\otimes H\otimes H\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) &= \frac{1}{4}[(|0\rangle + |1\rangle)\otimes(|0\rangle + |1\rangle)\otimes(|0\rangle + |1\rangle) \\
&+ (-1)^b(|0\rangle - |1\rangle)\otimes(|0\rangle - |1\rangle)\otimes(|0\rangle - |1\rangle)] \\
&= \frac{1}{4}[(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\
&+ (-1)^b(|000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle)]
\end{aligned}$$

So if $b = 0$, the state is now

$$\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$$

And if $b = 1$, the state is now

$$\frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$$

Now, Alice, Bob, and Charlie measure in the standard basis. We note that these three measurements are equivalent to a measurement in the computational in the product space. Thus, if $b = 0$, the only possible measurements for Alice, Bob, and, Charlie are $(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)$ If $b = 1$, the only possible measurements for Alice, Bob, and, Charlie are $(0, 0, 1), (0, 1, 0), (1, 0, 0), (1, 1, 1)$ Thus, to determine b, Bob and CHarlie send the bits from their measurements to Alice and Alice computes the parity of the three measurements, which is then equal to b.

Problem 4: Non-local boxes

Solution: (Due to De Huang)

(a) (U) For any input $(x, y) \in A_1 \times A_2$, we have

$$\sum_{a,b\in\{0,1\}} p(a, b|x, y) = 4 \times \frac{1}{4} = 1.$$

(PR) If $(x, y) \neq (1, 1)$,

$$\sum_{a,b\in\{0,1\}} p(a, b|x, y) = p(0, 0|x, y) + p(1, 1|x, y) = \frac{1}{2} + \frac{1}{2} = 1,$$

if $(x, y) = (1, 1)$,

$$\sum_{a,b\in\{0,1\}} p(a, b|x, y) = p(1, 0|x, y) + p(0, 1|x, y) = \frac{1}{2} + \frac{1}{2} = 1.$$

(CH) If $(x, y) \neq (1, 1)$,

$$\sum_{a,b\in\{0,1\}} p(a, b|x, y) = \frac{1}{2}\cos^2\frac{\pi}{8} + \frac{1}{2}\cos^2\frac{\pi}{8} + \frac{1}{2}\sin^2\frac{\pi}{8} + \frac{1}{2}\sin^2\frac{\pi}{8} = 1,$$

if $(x, y) = (1, 1)$,

$$\sum_{a,b\in\{0,1\}} p(a, b|x, y) = \frac{1}{2}\sin^2\frac{\pi}{8} + \frac{1}{2}\sin^2\frac{\pi}{8} + \frac{1}{2}\cos^2\frac{\pi}{8} + \frac{1}{2}\cos^2\frac{\pi}{8} = 1.$$

(SIG) For any input $(x, y) \in A_1 \times A_2$, we have

$$\sum_{a,b \in \{0,1\}} p(a, b|x, y) = p(y, x|x, y) = 1.$$

(b) Let

$$p(a, *|x, y) = \sum_{b \in \{0,1\}} p(a, b|x, y)$$

denote the marginal probability of the first output being a given the input (x, y), and

$$p(*, b|x, y) = \sum_{a \in \{0,1\}} p(a, b|x, y)$$

the marginal probability of the second output being b given the input (x, y).

(U) It's non-signaling, because

$$p(a, *|x, 0) = p(a, *|x, 1) = \frac{1}{2}, \quad \forall x \in \{0, 1\},\ \forall a \in \{0, 1\},$$

$$p(*, b|0, y) = p(*, b|1, y) = \frac{1}{2}, \quad \forall y \in \{0, 1\},\ \forall b \in \{0, 1\}.$$

(PR) It's non-signaling, because

$$p(a, *|x, y) = p(a, a \oplus (x \wedge y)|x, y) = \frac{1}{2}, \quad \forall x, y \in \{0, 1\},\ \forall a \in \{0, 1\},$$

$$p(*, b|x, y) = p(b \oplus (x \wedge y), b|x, y) = \frac{1}{2}, \quad \forall x, y \in \{0, 1\},\ \forall b \in \{0, 1\}.$$

(CH) It's non-signaling, because given any input (x, y), we always have

$$p(0, 0|x, y) = p(1, 1|x, y) = \frac{\neg(x \wedge y)}{2} \cos^2 \frac{\pi}{8} + \frac{x \wedge y}{2} \sin^2 \frac{\pi}{8},$$

$$p(1, 0|x, y) = p(0, 1|x, y) = \frac{x \wedge y}{2} \cos^2 \frac{\pi}{8} + \frac{\neg(x \wedge y)}{2} \sin^2 \frac{\pi}{8},$$

and thus

$$p(a, *|x, y) = p(a, 0|x, y) + p(a, 1|x, y) = \frac{1}{2}, \quad \forall x, y \in \{0, 1\},\ \forall a \in \{0, 1\},$$

$$p(*, b|x, y) = p(0, b|x, y) + p(1, b|x, y) = \frac{1}{2}, \quad \forall x, y \in \{0, 1\},\ \forall b \in \{0, 1\}.$$

(SIG) It's not non-signaling, because

$$p(1, *|0, 0) = 0, \quad p(1, *|0, 1) = p(1, 0|0, 1) = 1,$$

$$p(1, *|0, 0) \neq p(1, *|0, 1).$$

(c) We always have

$$\begin{aligned} p_{win} &= \sum_{x,y\in\{0,1\}} p(x,y)\Big(\sum_{a\oplus b = x\wedge y} p(a,b|x,y)\Big) \\ &= \frac{1}{4}(p(0,0|0,0)+p(1,1|0,0)) + \frac{1}{4}(p(0,0|0,1)+p(1,1|0,1)) \\ &\quad + \frac{1}{4}(p(0,0|1,0)+p(1,1|1,0)) + \frac{1}{4}(p(0,1|1,1)+p(1,0|1,1)). \end{aligned}$$

We just need to specify each probability for each cases.

(U) Everything is $\frac{1}{4}$, thus

$$p_{win} = \frac{1}{4}\times(\frac{1}{4}+\frac{1}{4})\times 4 = \frac{1}{2}.$$

(PR)

$$p_{win} = \frac{1}{4}\times(\frac{1}{2}+\frac{1}{2})\times 4 = 1.$$

(CH)

$$p_{win} = \frac{1}{4}\times(\frac{1}{2}\cos^2\frac{\pi}{8}+\frac{1}{2}\cos^2\frac{\pi}{8})\times 4 = \cos^2\frac{\pi}{8} = \frac{1}{2}+\frac{\sqrt{2}}{4}.$$

(SIG)

$$p_{win} = \frac{1}{4}p(0,0|0,0) = \frac{1}{4}.$$

(d) (U) Can. Let

$$\rho_{AB} = \frac{\mathbb{I}_2}{2}\otimes\frac{\mathbb{I}_2}{2},$$

$$A_0^0 = B_0^0 = |0\rangle\langle 0|, \quad A_0^1 = B_0^1 = |1\rangle\langle 1|, \quad A_1^0 = B_1^0 = |+\rangle\langle +|, \quad A_1^1 = B_1^1 = |-\rangle\langle -|.$$

It's easy to check that

$$tr\big((A_x^a\otimes B_y^b)\rho_{AB}\big) = \frac{1}{4}, \quad \forall x,y,a,b\in\{0,1\}.$$

(PR) Can not. We will prove by contradiction. For any POVM $\{A_x^0, A_x^1\}_a$, $x\in\{0,1\}$, $\{B_y^0, B_y^1\}_b$, $y\in\{0,1\}$, and any density matrix ρ_{AB}, consider the folloing formula

$$\begin{aligned} &(A_0^0 - A_0^1)\otimes(B_0^0 - B_0^1) + (A_0^0 - A_0^1)\otimes(B_1^0 - B_1^1) \\ &+ (A_1^0 - A_1^1)\otimes(B_0^0 - B_0^1) - (A_1^0 - A_1^1)\otimes(B_1^0 - B_1^1) \\ =\ & M_0N_0 + M_0N_1 + M_1N_0 - M_1N_1, \end{aligned}$$

where

$$M_i = (A_i^0 - A_i^1)\otimes\mathbb{I}_2, \quad N_i = \mathbb{I}_2\otimes B_i^0 - B_i^1, \quad i\in\{0,1\}.$$

It's easy to check that

$$-\mathbb{I}_4 \le M_i \le \mathbb{I}_4, \quad -\mathbb{I}_4 \le N_i \le \mathbb{I}_4,, \quad i =\in\{0,1\},$$

$$M_iN_j = N_jM_i, \quad i,j\in\{0,1\}.$$

Now define

$$\langle XY\rangle = tr(XY\rho_{AB}), \quad \langle X^2\rangle = \langle XX\rangle,$$

the we have

$$\langle M_iN_j\rangle = \langle N_jM_i\rangle, \quad i,j\in\{0,1\},$$

$$\langle(\sum_{i\in\{0,1\}}\alpha_iM_i + \sum_{j\in\{0,1\}}\beta_jN_j)^2\rangle \geq 0, \quad \forall \alpha_0,\alpha_1,\beta_0,\beta_1.$$

Then by direct calculation[1] , we have

$$\begin{aligned}
&tr\big((M_0N_0 + M_0N_1 + M_1N_0 - M_1N_1)\rho_{AB}\big)\\
&= \langle M_0N_0\rangle + \langle M_0N_1\rangle + \langle M_1N_0\rangle - \langle M_1N_1\rangle\\
&= \frac{1}{\sqrt{2}}\big(\langle M_0^2\rangle + \langle M_1^2\rangle + \langle N_0^2\rangle + \langle N_1^2\rangle\big)\\
&\quad - \frac{\sqrt{2}-1}{8}\langle\big((\sqrt{2}+1)(M_0-N_0)+M_1-N_1\big)^2\rangle - \frac{\sqrt{2}-1}{8}\langle\big((\sqrt{2}+1)(M_0-N_1)-M_1-N_0\big)^2\rangle\\
&\quad - \frac{\sqrt{2}-1}{8}\langle\big((\sqrt{2}+1)(M_1-N_0)+M_0+N_1\big)^2\rangle - \frac{\sqrt{2}-1}{8}\langle\big((\sqrt{2}+1)(M_1+N_1)-M_0-N_0\big)^2\rangle\\
&\leq \frac{1}{\sqrt{2}}\big(\langle M_0^2\rangle + \langle M_1^2\rangle + \langle N_0^2\rangle + \langle N_1^2\rangle\big)\\
&\leq \frac{1}{\sqrt{2}}\big(\langle \mathbb{I}_4\rangle + \langle \mathbb{I}_4\rangle + \langle \mathbb{I}_4\rangle + \langle \mathbb{I}_4\rangle\big)\\
&= 2\sqrt{2}.
\end{aligned}$$

However, if there exist such a quantum strategy that can implement (PR) box, than it's easy to check that

$$\begin{aligned}
&tr\big((M_0N_0 + M_0N_1 + M_1N_0 - M_1N_1)\rho_{AB}\big)\\
&= tr\big((A_0^0 - A_0^1)\otimes(B_0^0 - B_0^1))\rho_{AB}\big) + tr\big((A_0^0 - A_0^1)\otimes(B_1^0 - B_1^1)\rho_{AB}\big)\\
&\quad + tr\big((A_1^0 - A_1^1)\otimes(B_0^0 - B_0^1)\rho_{AB}\big) - tr\big((A_1^0 - A_1^1)\otimes(B_1^0 - B_1^1)\rho_{AB}\big)\\
&= 4,
\end{aligned}$$

which violates the upper bound $2\sqrt{2}$ we obtain above. This contradiction implies that we can not use quantum strategy to implement (PR) box.

(CH) Can. Let

$$\begin{aligned}
\rho_{AB} &= |EPR\rangle\langle EPR|_{AB}\\
&= \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)_{AB}\\
&= \frac{1}{2}(|+\rangle|+\rangle + |-\rangle|-\rangle)(\langle +|\langle +| + \langle -|\langle -|)_{AB},
\end{aligned}$$

$$A_0^0 = |0\rangle\langle 0|, \quad A_0^1 = |1\rangle\langle 1|, \quad A_1^0 = |+\rangle\langle +|, \quad A_1^1 = |-\rangle\langle -|,$$

[1] 1980 B.S. Cirel'son, ”Quantum generalizations of Bell's inequality.” Letters in Mathematical Physics 4, 93-100.

$$B_0^0 = |\phi_0\rangle\langle\phi_0|, \quad B_0^1 = |\phi_1\rangle\langle\phi_1|, \quad B_1^0 = |\psi_0\rangle\langle\psi_0|, \quad B_1^1 = |\psi_1\rangle\langle\psi_1|,$$

where

$$|\phi_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \quad |\phi_1\rangle = -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle,$$
$$|\psi_0\rangle = \cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle, \quad |\psi_1\rangle = \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle.$$

It's easy to check that

$$tr\big((A_x^a \otimes B_y^b)\rho_{AB}\big) = \frac{1}{2}\cos^2\frac{\pi}{8}, \quad \text{if} a \oplus b = x \wedge y,$$

$$tr\big((A_x^a \otimes B_y^b)\rho_{AB}\big) = \frac{1}{2}\sin^2\frac{\pi}{8}, \quad \text{if} a \oplus b \neq x \wedge y.$$

(SIG) Can not. We will show this by contradiction. Assume that there is such a strategy, then

$$tr\big((A_0^0 \otimes B_0^0)\rho_{AB}\big) = tr\big((A_1^1 \otimes B_1^1)\rho_{AB}\big) = 1,$$
$$tr\big((A_0^1 \otimes B_1^0)\rho_{AB}\big) = tr\big((A_1^0 \otimes B_0^1)\rho_{AB}\big) = 1.$$

In my HW3 problem 2, I have shown a lemma that if $X \geq Y,\ Z \geq 0$, then $tr(XZ) \geq tr(YZ)$. We will use this lemma here again. Since $\{A_x^a\}_a$ and $\{B_y^b\}_b$ are POVMs for all x, y, we have

$$\mathbb{I}_2 \geq B_0^0 \geq 0, \quad \mathbb{I}_2 \geq B_0^1 \geq 0,$$
$$A_0^0 \geq 0, \quad A_0^1 \geq 0, \quad A_0^0 + A_0^1 = \mathbb{I}_2,$$
$$\Longrightarrow \quad A_0^0 \otimes \mathbb{I}_2 \geq A_0^0 \otimes B_0^0 \geq 0, \quad A_0^1 \otimes \mathbb{I}_2 \geq A_0^1 \otimes B_1^0 \geq 0,$$
$$\Longrightarrow \quad \mathbb{I}_4 = \mathbb{I}_2 \otimes \mathbb{I}_2 = A_0^0 \otimes \mathbb{I}_2 + A_0^1 \otimes \mathbb{I}_2 \geq A_0^0 \otimes B_0^0 + A_0^1 \otimes B_1^0 \geq 0,$$

then using the lemma, we have

$$1 = tr(\mathbb{I}_4\rho_{AB}) \geq tr\big((A_0^0 \otimes B_0^0) + A_0^1 \otimes B_1^0)\rho_{AB}\big) = tr\big((A_0^0 \otimes B_0^0)\rho_{AB}\big) + tr\big((A_0^1 \otimes B_1^0)\rho_{AB}\big) = 2.$$

This contradiction implies that we can not find such a quantum strategy.

(e) Consider an non-signaling extension $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ of the (PR) box. Using non-signaling condition, we have

$$\sum_{a,b\in\{0,1\}} q(a,b,c|x,y,z) = \sum_{a,b\in\{0,1\}} q(a,b,c|x',y',z), \quad \forall c, z, \quad \forall x, y, x', y' \in \{0,1\},$$

therefore we can define

$$p'(c|z) = \sum_{a,b\in\{0,1\}} q(a,b,c|0,0,z) \geq 0, \quad \forall c, z,$$

then we have

$$p'(c|z) = \sum_{a,b\in\{0,1\}} q(a,b,c|x,y,z), \quad \forall x, y \in \{0,1\}.$$

Also we can check that for all z,

$$\sum_c p'(c,z) = \sum_{a,b\in\{0,1\}} \sum_c q(a,b,c|0,0,z) = \sum_{a,b\in\{0,1\}} p(a,b|0,0) = 1,$$

thus $\{p'(c|z)\}_z$ is a family of well defined distributions. Now using the properties of (PR) box, we have

$$\begin{aligned}
&\sum_c q(0,1,c|x,y,z) = p(0,1|x,y) = 0,\ \forall z, \quad \text{if } (x,y) \neq (1,1),\\
&\sum_c q(1,0,c|x,y,z) = p(1,0|x,y) = 0,\ \forall z, \quad \text{if } (x,y) \neq (1,1),\\
&\sum_c q(0,0,c|x,y,z) = p(0,0|x,y) = 0,\ \forall z, \quad \text{if } (x,y) = (1,1),\\
&\sum_c q(1,1,c|x,y,z) = p(1,1|x,y) = 0,\ \forall z. \quad \text{if } (x,y) = (1,1),
\end{aligned}$$

Since all probabilities are non negative, we have

$$\begin{aligned}
q(0,1,c|x,y,z) &= 0 = p(0,1|x,y)p'(c|z),\ \forall c,z, \quad \text{if } (x,y) \neq (1,1),\\
q(1,0,c|x,y,z) &= 0 = p(1,0|x,y)p'(c|z),\ \forall c,z, \quad \text{if } (x,y) \neq (1,1),\\
q(0,0,c|x,y,z) &= 0 = p(0,0|x,y)p'(c|z),\ \forall c,z, \quad \text{if } (x,y) = (1,1),\\
q(1,1,c|x,y,z) &= 0 = p(1,1|x,y)p'(c|z),\ \forall c,z, \quad \text{if } (x,y) = (1,1).
\end{aligned}$$

Then using the non-signaling condition for fixing two inputs and outputs, we have

$$q(0,0,c|0,0,z) = q(0,0,c|0,1,z) = q(1,0,c|1,1,z) = q(1,1,c|1,0,z) = q(1,1,c|0,0,z),\ \forall c,z,$$

and since we also have

$$\sum_{a,b\in\{0,1\}} q(a,b,c|0,0,z) = q(0,0,c|0,0,z) + q(1,1,c|0,0,z) = p'(c|z),\ \forall c,z,$$

thus

$$\begin{aligned}
q(0,0,c|0,0,z) &= \frac{1}{2}p'(c|z) = p(0,0|0,0)p'(c,z),\ \forall c,z,\\
q(1,1,c|0,0,z) &= \frac{1}{2}p'(c|z) = p(1,1|0,0)p'(c,z),\ \forall c,z.
\end{aligned}$$

Similarly we can also prove that

$$\begin{aligned}
q(0,0,c|x,y,z) &= \frac{1}{2}p'(c|z) = p(0,0|x,y)p'(c,z), \forall c,z, \quad \text{if } (x,y) \neq (1,1),\\
q(1,1,c|x,y,z) &= \frac{1}{2}p'(c|z) = p(1,1|x,y)p'(c,z), \forall c,z, \quad \text{if } (x,y) \neq (1,1),\\
q(0,1,c|x,y,z) &= \frac{1}{2}p'(c|z) = p(0,1|x,y)p'(c,z), \forall c,z, \quad \text{if } (x,y) = (1,1),\\
q(1,0,c|x,y,z) &= \frac{1}{2}p'(c|z) = p(1,0|x,y)p'(c,z), \forall c,z, \quad \text{if } (x,y) = (1,1).
\end{aligned}$$

Therefore the extension $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ is in a product form.

(f) Let $c \in \mathcal{X}_3 = \{0,1\}$, $z \in \mathcal{A}_3 = \{0\}$. Let

$$\begin{cases} q(0,0,0|x,y,z) = q(1,1,0|x,y,z) = \frac{1}{4}, \\ q(0,0,1|x,y,z) = q(1,1,1|x,y,z) = \frac{1}{2}\cos\frac{\pi}{8}\sin\frac{\pi}{8}, \\ q(1,0,1|x,y,z) = q(0,1,1|x,y,z) = \frac{1}{4}\sin^2\frac{\pi}{8}, \\ q(1,0,0|x,y,z) = q(0,1,0|x,y,z) = \frac{1}{4}\sin^2\frac{\pi}{8}, \end{cases} \quad \text{if } (x,y) \neq (1,1),$$

$$\begin{cases} q(0,0,0|x,y,z) = q(1,1,0|x,y,z) = \frac{1}{4}\sin^2\frac{\pi}{8}, \\ q(0,0,1|x,y,z) = q(1,1,1|x,y,z) = \frac{1}{4}\sin^2\frac{\pi}{8}, \\ q(1,0,1|x,y,z) = q(0,1,1|x,y,z) = \frac{1}{2}\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \\ q(1,0,0|x,y,z) = q(0,1,0|x,y,z) = \frac{1}{4}, \end{cases} \quad \text{if } (x,y) = (1,1).$$

It's easy to check that this $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ defines a tripartite non local box. Also, using the fact that

$$\frac{1}{2} + \cos\frac{\pi}{8}\sin\frac{\pi}{8} = \cos^2\frac{\pi}{8},$$

and noticing that z is always 0, we can check that

$$\sum_{b,c} q(a,b,c|x,y,0) = \sum_{b,c} q(a,b,c|x,y',0), \quad \forall a,x,y,y',$$

$$\sum_{a,c} q(a,b,c|x,y,0) = \sum_{a,c} q(a,b,c|x',y,0), \quad \forall b,x,y,x',$$

$$\sum_{a,b} q(a,b,c|x,y,0) = \sum_{a,b} q(a,b,c|x',y',0), \quad \forall a,x,y,x',y',$$

$$\sum_{b} q(a,b,c|x,y,0) = \sum_{b} q(a,b,c|x,y',0), \quad \forall a,c,x,y,y',$$

$$\sum_{a} q(a,b,c|x,y,0) = \sum_{a} q(a,b,c|x',y,0), \quad \forall b,c,x,y,x',$$

therefore it's non-signaling. Moreover, if $(x,y) \neq (1,1)$ we have

$$\sum_{c\in\{0,1\}} q(0,0,c|x,y,z) = \frac{1}{2}\cos^2\frac{\pi}{8} = p(0,0|x,y), \quad \sum_{c\in\{0,1\}} q(1,1,c|x,y,z) = \frac{1}{2}\cos^2\frac{\pi}{8} = p(1,1|x,y),$$

$$\sum_{c\in\{0,1\}} q(1,0,c|x,y,z) = \frac{1}{2}\sin^2\frac{\pi}{8} = p(1,0|x,y), \quad \sum_{c\in\{0,1\}} q(0,1,c|x,y,z) = \frac{1}{2}\sin^2\frac{\pi}{8} = p(0,1|x,y),$$

if $(x,y) = (1,1)$ we have

$$\sum_{c\in\{0,1\}} q(0,0,c|x,y,z) = \frac{1}{2}\sin^2\frac{\pi}{8} = p(0,0|x,y), \quad \sum_{c\in\{0,1\}} q(1,1,c|x,y,z) = \frac{1}{2}\sin^2\frac{\pi}{8} = p(1,1|x,y),$$

$$\sum_{c\in\{0,1\}} q(1,0,c|x,y,z) = \frac{1}{2}\cos^2\frac{\pi}{8} = p(1,0|x,y), \qquad \sum_{c\in\{0,1\}} q(0,1,c|x,y,z) = \frac{1}{2}\cos^2\frac{\pi}{8} = p(0,1|x,y).$$

Therefore this $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ is a non-signaling extension of (CH) box.

However, if this $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ has a product form, then we have

$$q(0,0,0|0,0,z) = p(0,0|0,0)p'(0|z) \quad\Longrightarrow\quad p'(0|z) = \frac{q(0,0,0|0,0,z)}{p(0,0|0,0)} = \frac{1}{2\cos^2\frac{\pi}{8}},$$

$$q(0,0,0|1,1,z) = p(0,0|1,1)p'(0|z) \quad\Longrightarrow\quad p'(0|z) = \frac{q(0,0,0|1,1,z)}{p(0,0|1,1)} = \frac{1}{2}.$$

This contraction implies that this $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ is a non-product, non-signaling extension of (CH) box.

(g) Given that each pair is chosen uniformly and (x,y,z) is generated uniformly, the success probability is

$$\begin{aligned}\mathbf{Pr}_{win} &= \frac{1}{3}\sum_{x,y,z\in\{0,1\}}\frac{1}{8}\Big(\sum_{a\oplus b=x\wedge y} p(a,b,c|x,y,z) + \sum_{a\oplus c=x\wedge z} p(a,b,c|x,y,z) + \sum_{b\oplus c=y\wedge z} p(a,b,c|x,y,z)\Big)\\ &= \frac{1}{24}\sum_{x,y,z\in\{0,1\}}\Big(\sum_{a\oplus b=x\wedge y} p(a,b,c|x,y,z) + \sum_{a\oplus c=x\wedge z} p(a,b,c|x,y,z) + \sum_{b\oplus c=y\wedge z} p(a,b,c|x,y,z)\Big)\\ &= \frac{1}{24}\sum_{x,y,z\in\{0,1\}}\Big(I_1(x,y,z) + I_2(x,y,z) + I_3(x,y,z)\Big),\end{aligned}$$

where $I_i(x,y,z),\ i=1,2,3$ denote the success probability under the condition that the input is (x,y,z) and the i_{th} pair is chosen. Here the first, second and third pair means (A,B), (A,C) and (B,C) respectively.

The following table gives occurrence number of each term $p(a,b,c|x,y,z)$ in the summation $I_1(x,y,z)+I_2(x,y,z)+I_3(x,y,z)$.

xyz

		000	100	010	001	011	101	110	111
abc	000	3	3	3	3	2	2	2	0
	001	1	1	1	1	2	2	0	2
	010	1	1	1	1	2	0	2	2
	100	1	1	1	1	0	2	2	2
	011	1	1	1	1	0	2	2	2
	101	1	1	1	1	2	0	2	2
	110	1	1	1	1	2	2	0	2
	111	3	3	3	3	2	2	2	0

Using this table and the condition that

$$\sum_{a,b,c\{0,1\}} p(a,b,c|x,y,z) = 1, \quad \forall x,y,z,$$

we can easily see that

$$\begin{aligned}
\mathbf{Pr}_{win} &= \frac{1}{24}\big(12 + 2p(0,0,0|0,0,0) + 2p(0,0,0|1,0,0) + 2p(0,0,0|0,1,0) + 2p(0,0,0|0,0,1) \\
&\qquad + 2p(1,1,1|0,0,0) + 2p(1,1,1|1,0,0) + 2p(1,1,1|0,1,0) + 2p(1,1,1|0,0,1) \\
&\qquad - 2p(1,0,0|0,1,1) - 2p(0,1,0|1,0,1) - 2p(0,0,1|1,1,0) - 2p(0,0,0|1,1,1) \\
&\qquad - 2p(0,1,1|0,1,1) - 2p(1,0,1|1,0,1) - 2p(1,1,0|1,1,0) - 2p(1,1,1|1,1,1)\big) \\
&\le \frac{1}{24}\big(12 + 2p(0,0,0|0,0,0) + 2p(0,0,0|1,0,0) + 2p(0,0,0|0,1,0) + 2p(0,0,0|0,0,1) \\
&\qquad + 2p(1,1,1|0,0,0) + 2p(1,1,1|1,0,0) + 2p(1,1,1|0,1,0) + 2p(1,1,1|0,0,1) \\
&\qquad - 2p(0,0,0|1,1,1) - 2p(1,1,1|1,1,1)\big).
\end{aligned}$$

Notice that whichever pair of players is chosen, (a,b,c) is a valid answer to the input (x,y,z) if and only if $(a\oplus 1, b\oplus 1, c\oplus 1)$ is a valid answer to (x,y,z). Therefore, given a tripartite box $\{p(\cdot,\cdot,\cdot|x,y,z)\}$, if we define a new tripartite $\{q(\cdot,\cdot,\cdot|x,y,z)\}$ box like

$$q(a,b,c|x,y,z) = \frac{1}{2}\big(p(a,b,c|x,y,z) + p(a\oplus 1, b\oplus 1, c\oplus 1|x,y,z)\big), \quad \forall a,b,c,x,y,z,$$

then it's easy to check that we will have

$$\mathbf{Pr}_{win}(p) = \mathbf{Pr}_{win}(q),$$

that is to say such transformation preserves the success probability. Also if $\{p(\cdot,\cdot,\cdot|x,y,z)\}$ is non-signaling, then for any (a,x), we have

$$\begin{aligned}
\sum_{b,c\in\{0,1\}} q(a,b,c|x,y,z) &= \frac{1}{2}\sum_{b,c\in\{0,1\}} \big(p(a,b,c|x,y,z) + p(a\oplus 1, b\oplus 1, c\oplus 1|x,y,z)\big) \\
&= \frac{1}{2}\sum_{b,c\in\{0,1\}} \big(p(a,b,c|x,y',z') + p(a\oplus 1, b\oplus 1, c\oplus 1|x,y',z')\big) \\
&= \sum_{b,c\in\{0,1\}} q(a,b,c|x,y',z'), \quad \forall y,z,y'z',
\end{aligned}$$

and this is also true for any (b,y) or any (c,z). Also for any (a,b,x,y), we have

$$\begin{aligned}
\sum_{c\in\{0,1\}} q(a,b,c|x,y,z) &= \frac{1}{2}\sum_{c\in\{0,1\}} \big(p(a,b,c|x,y,z) + p(a\oplus 1, b\oplus 1, c\oplus 1|x,y,z)\big) \\
&= \frac{1}{2}\sum_{c\in\{0,1\}} \big(p(a,b,c|x,y,z') + p(a\oplus 1, b\oplus 1, c\oplus 1|x,y,z')\big) \\
&= \sum_{c\in\{0,1\}} q(a,b,c|x,y,z'), \quad \forall z,z',
\end{aligned}$$

and this is true for any (a, c, x, z) or any (b, c, y, z). Therefor $\{q(\cdot, \cdot, \cdot|x, y, z)\}$ is also non-signaling. Thus this transformation transformation also preserves the non-signaling property. Out of this reason, from now on we can alwasy assume that

$$p(a, b, c|x, y, z) = p(a \oplus 1, b \oplus 1, c \oplus 1|x, y, z)\big), \quad \forall a, b, c, x, y, z, \tag{$*$}$$

otherwise we can do this transformation to $\{p(\cdot, \cdot, \cdot|x, y, z)\}$ to make it so.

Now we continue our task of finding the upper bound of success probability,

$$\begin{aligned}
\mathbf{Pr}_{win} \le \frac{1}{24}\big(&12 + 2p(0,0,0|0,0,0) + 2p(0,0,0|1,0,0) + 2p(0,0,0|0,1,0) + 2p(0,0,0|0,0,1) \\
&+ 2p(1,1,1|0,0,0) + 2p(1,1,1|1,0,0) + 2p(1,1,1|0,1,0) + 2p(1,1,1|0,0,1) \\
&- 2p(0,0,0|1,1,1) - 2p(1,1,1|1,1,1)\big) \\
= \frac{1}{24}\big(&12 + 4p(0,0,0|0,0,0) + 4p(0,0,0|1,0,0) + 4p(0,0,0|0,1,0) + 4p(0,0,0|0,0,1) \\
&- 4p(0,0,0|1,1,1)\big) \\
= \frac{1}{2} + \frac{1}{6}\big(&p(0,0,0|0,0,0) + p(0,0,0|1,0,0) + p(0,0,0|0,1,0) + p(0,0,0|0,0,1) \\
&- p(0,0,0|1,1,1)\big),
\end{aligned}$$

where we have used the condition $(*)$. Next we will have to do some painful calculation. Using condition $(*)$ and non-signaling condition for fixing two inputs, we can show that

$$p(0,0,1|0,1,1) + p(0,1,0|0,1,1) = p(0,0,1|1,1,1) + p(0,1,0|1,1,1),$$

$$p(0,0,1|1,0,1) + p(1,0,0|1,0,1) = p(0,0,1|1,1,1) + p(1,0,0|1,1,1),$$
$$p(0,1,0|1,1,0) + p(1,0,0|1,1,0) = p(0,1,0|1,1,1) + p(1,0,0|1,1,1),$$

$$\begin{aligned}
\Longrightarrow \quad & p(0,0,1|0,1,1) + p(0,1,0|0,1,1) + p(0,0,1|1,0,1) \\
& + p(1,0,0|1,0,1) + p(0,1,0|1,1,0) + p(1,0,0|1,1,0) \\
= {} & 2p(0,0,1|1,1,1) + 2p(0,1,0|1,1,1) + 2p(1,0,0|1,1,1) \\
= {} & 1 - 2p(0,0,0|1,1,1).
\end{aligned}$$

On the other hand, still using condition $(*)$ and non-signaling condition for fixing two inputs, we can check that

$$\begin{aligned}
& p(0,0,1|1,0,0) + p(0,1,0|1,0,0) + 2p(1,0,0|1,0,0) \\
& + p(0,0,1|0,1,0) + 2p(0,1,0|0,1,0) + p(1,0,0|0,1,0) \\
& + 2p(0,0,1|0,0,1) + p(0,1,0|0,0,1) + p(1,0,0|0,0,1) \\
= {} & p(0,0,1|0,1,1) + p(0,1,0|0,1,1) + p(0,0,1|1,0,1) \\
& + p(1,0,0|1,0,1) + p(0,1,0|1,1,0) + p(1,0,0|1,1,0) \\
& + 2p(1,0,0|0,1,1) + 2p(0,1,0|1,0,1) + 2p(0,0,1|1,1,0) \\
= {} & 1 - 2p(0,0,0|1,1,1) \\
& + 2p(1,0,0|0,1,1) + 2p(0,1,0|1,0,1) + 2p(0,0,1|1,1,0)
\end{aligned}$$

Notice that condition $(*)$ gives

$$\begin{aligned}&2p(0,0,0|1,0,0)+2p(0,0,0|0,1,0)+2p(0,0,0|0,0,1)\\&+p(0,0,1|1,0,0)+p(0,1,0|1,0,0)+2p(1,0,0|1,0,0)\\&+p(0,0,1|0,1,0)+2p(0,1,0|0,1,0)+p(1,0,0|0,1,0)\\&+2p(0,0,1|0,0,1)+p(0,1,0|0,0,1)+p(1,0,0|0,0,1)\le 3,\end{aligned}$$

thus

$$\begin{aligned}&2p(0,0,0|1,0,0)+2p(0,0,0|0,1,0)+2p(0,0,0|0,0,1)\\&+1-2p(0,0,0|1,1,1)\\&+2p(1,0,0|0,1,1)+2p(0,1,0|1,0,1)+2p(0,0,1|1,1,0)\le 3,\end{aligned}$$

$$\begin{aligned}\Longrightarrow\quad &p(0,0,0|1,0,0)+p(0,0,0|0,1,0)+p(0,0,0|0,0,1)-p(0,0,0|1,1,1)\\ \le\ &1-p(1,0,0|0,1,1)-p(0,1,0|1,0,1)-p(0,0,1|1,1,0)\\ \le\ &1.\end{aligned}$$

Finally we have

$$\begin{aligned}\mathbf{Pr}_{win}&\le\frac{1}{2}+\frac{1}{6}\big(p(0,0,0|0,0,0)+p(0,0,0|1,0,0)+p(0,0,0|0,1,0)+p(0,0,0|0,0,1)\\&\qquad\qquad-p(0,0,0|1,1,1)\big)\\&\le\frac{1}{2}+\frac{1}{6}\big(p(0,0,0|0,0,0)+1\big)\\&\le\frac{1}{2}+\frac{1}{6}\big(\frac{1}{2}+1\big)\\&=\frac{3}{4}.\end{aligned}$$

Here we have used the condition $(*)$, so $p(0,0,0|0,0,0)\le\frac{1}{2}$.

Now we have proved that $\frac{3}{4}$ is a upper bound of the success probability. Indeed if we take

$$p(0,0,0|x,y,z)=p(1,1,1|x,y,z)=\frac{1}{2},\quad\forall x,y,z,$$

and all unspecified probabilities being 0, then we can check that this $\{p(\cdot,\cdot,\cdot|x,y,z)\}$ is a non-signaling tripartite nonlocal box, and we have

$$\begin{aligned}\mathbf{Pr}_{win}&=\frac{1}{24}\big(12+2p(0,0,0|0,0,0)+2p(0,0,0|1,0,0)+2p(0,0,0|0,1,0)+2p(0,0,0|0,0,1)\\&\qquad+2p(1,1,1|0,0,0)+2p(1,1,1|1,0,0)+2p(1,1,1|0,1,0)+2p(1,1,1|0,0,1)\\&\qquad-2p(0,0,0|1,1,1)-2p(1,1,1|1,1,1)\big)\\&=\frac{3}{4}.\end{aligned}$$

Therefore the optimum success probability achieved by any non-signaling tripartite box in this game is $\frac{3}{4}$.