CS/Ph120 Homework 6 Solutions

November 18, 2016

Problem 1: The Pretty-Good-Measurement is not Optimal

Solution: (Due to De Huang)

(a) We have

$$\rho = \frac{1}{3}(\rho_0 + \rho_1 + \rho_2) = \frac{1}{2}\mathbb{I}, \quad \rho^{-\frac{1}{2}} = \sqrt{2}\mathbb{I},$$

thus the pretty-good-measurement $\{M_0, M_1, M_2\}$ is give by

$$M_0 = \frac{1}{3}\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}} = \frac{2}{3}|0\rangle\langle 0|, \quad M_1 = \frac{1}{3}\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}} = \frac{1}{3}\mathbb{I}, \quad M_2 = \frac{1}{3}\rho^{-\frac{1}{2}}\rho_2\rho^{-\frac{1}{2}} = \frac{2}{3}|1\rangle\langle 1|,$$

and the success probability using this measurement is

$$p_{good} = \frac{1}{3}\big(tr(M_0\rho_0) + tr(M_1\rho_1) + tr(M_2\rho_2)\big) = \frac{5}{9}.$$

(b) Let $\sigma^* = \frac{1}{3}\mathbb{I}$, then it's easy to check that

$$\sigma^* \geq \frac{1}{3}|0\rangle\langle 0| = p_0\rho_0, \quad \sigma^* \geq \frac{1}{3} \times \frac{1}{2}\mathbb{I} = p_1\rho_1, \quad \sigma^* \geq \frac{1}{3}|1\rangle\langle 1| = p_2\rho_2,$$

therefore

$$P_{guess} = \inf_{\sigma \geq p_i\rho_i, i=0,1,2} tr(\sigma) \leq tr(\sigma^*) = \frac{2}{3}.$$

$\frac{2}{3}$ is an upper bound of the guessing probability. We will show that this is actually the maximum of the guessing probability. Indeed, consider a POVM $\{M_0^*, M_1^*, M_2^*\}$,

$$M_0^* = |0\rangle\langle 0|, \quad M_1^* = 0, \quad M_2^* = |1\rangle\langle 1|.$$

We can check that this is a legal POVM, and the success probability using this POVM is

$$p_{succ}^* = \frac{1}{3}\big(tr(M_0^*\rho_0) + tr(M_1^*\rho_1) + tr(M_2^*\rho_2)\big) = \frac{2}{3}.$$

Thus we have

$$\frac{2}{3} \geq P_{guess} \geq p_{succ}^* = \frac{2}{3},$$

which implies $P_{guess} = \frac{2}{3}$.

(c) Already done in (b).

Problem 2: Properties of the Pretty-Good-Measurement

Solution: (Due to De Huang)

(a) Suppose $\rho = p_0\rho_0 + p_1\rho_1,\ p_0, p_1 \geq 0,\ p_0 + p_1 = 1$, then the pretty-good-measurement is given by

$$M_0 = \rho^{-\frac{1}{2}} p_0\rho_0\rho^{-\frac{1}{2}}, \quad M_1 = \rho^{-\frac{1}{2}} p_1\rho_1\rho^{-\frac{1}{2}}.$$

We only need to show that

$$tr(M_0\rho_0) \geq tr(M_0\rho_1), \quad tr(M_1\rho_1) \geq tr(M_1\rho_0).$$

Define

$$a = tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}\rho_0), \quad b = tr(\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}}\rho_1), \quad c = tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}\rho_1).$$

It's easy to check that $a, b, c \geq 0$, and we have

$$\begin{cases} p_0 a + p_1 c = tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}p_0\rho_0) + tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}p_1\rho_1) = tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}\rho) = tr(\rho_0) = 1, \\ p_0 c + p_1 b = tr(\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}}p_0\rho_0) + tr(\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}}p_1\rho_1) = tr(\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}}\rho) = tr(\rho_1) = 1, \end{cases}$$

$$\Longrightarrow \quad p_0(a-c) = p_1(b-c).$$

Also using Cauchy-Schwarz inequality we have

$$\begin{aligned} c^2 &= \Big(tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}\rho_1)\Big)^2 \\ &= \Big(tr(\rho^{-\frac{1}{4}}\rho_0\rho^{-\frac{1}{4}}\rho^{-\frac{1}{4}}\rho_1\rho^{-\frac{1}{4}})\Big)^2 \\ &\leq \Big(tr(\rho^{-\frac{1}{4}}\rho_0\rho^{-\frac{1}{4}}\rho^{-\frac{1}{4}}\rho_0\rho^{-\frac{1}{4}})\Big)\Big(tr(\rho^{-\frac{1}{4}}\rho_1\rho^{-\frac{1}{4}}\rho^{-\frac{1}{4}}\rho_1\rho^{-\frac{1}{4}})\Big) \\ &= tr(\rho^{-\frac{1}{2}}\rho_0\rho^{-\frac{1}{2}}\rho_0)tr(\rho^{-\frac{1}{2}}\rho_1\rho^{-\frac{1}{2}}\rho_1) \\ &= ab. \end{aligned}$$

That is to say, at least one of the following is true: $a \geq c$; $b \geq c$. Then using $p_0(a-c) = p_1(b-c)$, we must have

$$p_0(a-c) = p_1(b-c) \geq 0.$$

Therefore

$$tr(M_0\rho_0) = tr(\rho^{-\frac{1}{2}}p_0\rho_0\rho^{-\frac{1}{2}}\rho_0) = p_0 a \geq p_0 c = tr(\rho^{-\frac{1}{2}}p_0\rho_0\rho^{-\frac{1}{2}}\rho_1) = tr(M_0\rho_1),$$

$$tr(M_1\rho_1) = tr(\rho^{-\frac{1}{2}}p_1\rho_1\rho^{-\frac{1}{2}}\rho_1) = p_1 b \geq p_1 c = tr(\rho^{-\frac{1}{2}}p_1\rho_1\rho^{-\frac{1}{2}}\rho_0) = tr(M_1\rho_0).$$

(b) In this case, we have

$$\rho = \frac{2}{5}\rho_0 + \frac{2}{5}\rho_1 + \frac{1}{5}\rho_2 = \frac{1}{5}\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \quad \rho^{-\frac{1}{2}} = \sqrt{5}\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} \end{pmatrix},$$

and the pretty-good-measurement is given by

$$M_0 = \begin{pmatrix} \frac{2}{3} & 0 \\ 0 & \frac{2}{9} \end{pmatrix}, \quad M_1 = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{4}{9} \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}.$$

We can see check that

$$tr(M_1\rho_1) = \frac{1}{3} \times (\frac{1}{3} + \frac{8}{9}) = \frac{11}{27}, \quad tr(M_1\rho_2) = \frac{4}{9} = \frac{12}{27},$$

$$tr(M_1\rho_1) < tr(M_1\rho_2),$$

which violates inequality (2).

Problem 3: Deterministic Extractors on Bit-Fixing Sources.

Solution: (Due to Bolton Bailey)

(a) The min entropy for X is defined

$$H_{\min}(X) = -\log \max p_x$$

Since each of the last $n - t$ bits of X_0 is uniformly random and independent of the other bits, there are 2^{n-t} equally likely outcomes for the distribution X_0, so

$$H_{\min}(X_0) = -\log \max \frac{1}{2^{n-t}} = -\log \frac{1}{2^{n-t}} = n - t$$

For X_1, there are 2^{n-1} strings of length $n - 1$, and for each of these, there is exactly one bit we can append to get a string with an even number of 0s. Thus X_1 has 2^{n-1} equally likely outcomes.

$$H_{\min}(X_0) = -\log \max \frac{1}{2^{n-1}} = -\log \frac{1}{2^{n-1}} = n - 1$$

For X_2, there are $2^{n/2}$ possiblitilites for the first half of the string, and since the first half of the string determines the second half, there are $2^{n/2}$ equally likely outcomes.

$$H_{\min}(X_0) = -\log \max \frac{1}{2^{n/2}} = -\log \frac{1}{2^{n/2}} = n/2$$

(b) $f_0(X_0)$ is not uniformly random, since this is the XOR of t 1s, so this always produces t mod 2.

$f_0(X_1)$ is uniformly random, since $t < n$, so the first t bits of n are uniformly random, so their XOR is uniformly random. (Unless $t = 0$ in which case the output is not uniform random, it is 0)

$f_0(X_2)$ is uniformly random, since if $1 \leq t \leq n/2$, it is the XOR of the first t bits of the string and if $n/2 \leq t \leq n$, it is the XOR of the last $n - t$ bits of a unform string. (Unless $t = 0$ in which case the output is not uniform random, it is 0)

$f_1(X_0)$ is uniformly random, since if $1 \leq t \leq n/2$, then $x_1 x_{1+n/2}$ is uniform random, and if $n/2 \leq t < n$, then $x_{n/2} x_n$ is uniform random.

$f_1(X_1)$ is uniformly random only if $n/2$ is odd. If the first half of x has at least a 0 and at least a 1, then there is a $1/2$ chance of each outcome, since if we choose the corresponding elements of the right half last, we can get either a result of 0 or 1. (TAs comment: In other

words, for any possible string on the other $n-4$ bits, we can always make the value of $f_1(X_1) = 1$ by choosing appropriately the bit in the second half that is multiplied with the 1, and fix the number of zeros to be even by choosing appropriately the bit in the second half that is multiplied with 0). If the first half is all 0s, the result will be 0. If The first half is all 1s, then the result is the parity of the second half, which is 1 only if $n/2$ is odd.

$f_1(X_2)$ is uniformly random, since it is the XOR of a uniform random string of length $n/2$

$f_2(X_0)$ is uniformly random, since the last bit is always uniformly random and independent of the previous bits.

$f_2(X_1)$ is not uniformly random, since if there are an even number of 0s, since n is even, there is an even number of 1s, so the XOR is 0.

$f_2(X_2)$ is not uniformly random, since the XOR of the whole string is the XOR of the first and second halves, which have the same parity, so this always results in 0.

(c) Consider the function f defined as follows: We divide the input x into $\lfloor \frac{n}{t+1} \rfloor$ disjoint segments each containing $t+1$ bits. There will always be enough bits to do this since

$$\lfloor \frac{n}{t+1} \rfloor \leq \frac{n}{t+1}$$

$$(t+1) \cdot \lfloor \frac{n}{t+1} \rfloor \leq (t+1) \cdot \frac{n}{t+1} = n$$

If there are leftover bits we ignore them. We then define $f(x)$ such that the ith bit of $f(x)$ is equal to the XOR of the ith segment (this means the outputs will have the correct number of bits, the same as the number of segments). Moreover, since Eve has only t bits, and the segments are $t+1$ bits, Eve never has all the bits in a segment, and the ith bit of the output is therefore independent of Eve. Thus, the whole output is independent of Eve.

Problem 4: No Chain Rule for Conditional Min-Entropy

Solution: (Due to De Huang)

(a)

$$\begin{aligned}
H(Y|X) &= \sum_x \mathbf{Pr}[X=x] H(Y|X=x) \\
&= \sum_x \mathbf{Pr}[X=x] \sum_y \mathbf{Pr}[Y=y|X=x] \log(\frac{1}{\mathbf{Pr}[Y=y|X=x]}) \\
&= \sum_x \mathbf{Pr}[X=x] \sum_y \frac{\mathbf{Pr}[Y=y, X=x]}{\mathbf{Pr}[X=x]} \log(\frac{\mathbf{Pr}[X=x]}{\mathbf{Pr}[Y=y, X=x]}) \\
&= \sum_x \sum_y \mathbf{Pr}[Y=y, X=x] \Big(\log(\frac{1}{\mathbf{Pr}[Y=y, X=x]}) - \log(\frac{1}{\mathbf{Pr}[X=x]}) \Big) \\
&= \sum_x \sum_y \mathbf{Pr}[Y=y, X=x] \log(\frac{1}{\mathbf{Pr}[Y=y, X=x]}) \\
&\quad - \sum_x \sum_y \mathbf{Pr}[Y=y, X=x] \log(\frac{1}{\mathbf{Pr}[X=x]}) \\
&= H(XY) - \sum_x \mathbf{Pr}[X=x] \log(\frac{1}{\mathbf{Pr}[X=x]}) \\
&= H(XY) - H(X).
\end{aligned}$$

(b) Given that X and Y are independent, we have

$$\begin{aligned}
H_{min}(XY) &= -\log P_{guess}(XY) \\
&= -\log(P_{guess}(X) P_{guess}(Y)) \\
&= -\log P_{guess}(X) - \log P_{guess}(Y) \\
&= H(X) + H(Y),
\end{aligned}$$

and thus

$$H(Y|X) = H(Y) = H(XY) - H(X).$$

(c) For $i = 1$,

$$P_{guess}(X_1) = \mathbf{Pr}[X_1 = 0] = \frac{5}{8}, \quad P_{guess}(X_1 Y_1) = \mathbf{Pr}[X_1 Y_1 = 00] = \frac{1}{2},$$

$$P_{guess}(Y_1|X_1) = \mathbf{Pr}[X=0]\mathbf{Pr}[Y_1=0|X_1=0] + \mathbf{Pr}[X_1=1]\mathbf{Pr}[Y_1=0|X_1=1] = \frac{3}{4},$$

$$H_{min}(X_1) = -\log\frac{5}{8} = 3 - \log 5, \quad H_{min}(X_1 Y_1) = -\log\frac{1}{2} = 1,$$

$$H_{min}(Y_1|X_1) = -\log\frac{3}{4} = 2 - \log 3,$$

$$H_{min}(Y_1|X_1) > H_{min}(X_1 Y_1) - H_{min}(X_1).$$

For $i = 2$,

$$P_{guess}(X_2) = \mathbf{Pr}[X_2 = 0] = \frac{5}{8}, \quad P_{guess}(X_2 Y_2) = \mathbf{Pr}[X_2 Y_2 = 00] = \frac{3}{8},$$

$$P_{guess}(Y_2|X_2) = \mathbf{Pr}[X_2 = 0]\mathbf{Pr}[Y_2 = 0|X_2 = 0] + \mathbf{Pr}[X = 1]\mathbf{Pr}[Y_2 = 0|X_2 = 1] = \frac{11}{16},$$

$$H_{min}(X_2) = -\log\frac{5}{8} = 3 - \log 5, \quad H_{min}(X_2Y_2) = -\log\frac{3}{8} = 3 - \log 3,$$

$$H_{min}(Y_2|X_2) = -\log\frac{11}{16} = 4 - \log 11,$$

$$H_{min}(Y_2|X_2) < H_{min}(X_2Y_2) - H_{min}(X_2).$$

We have encountered all cases where $H_{min}(Y|X) =, >, < H_{min}(XY) - H_{min}(X)$, thus we may conclude that there is no certain form of the chain rule for conditional min-entropy.

Problem 5: Optimal qubit strategies in the CHSH game.

Solution: (Due to Bolton Bailey)

(a) We wish to show that any observable O is of the form

$$O = \alpha X + \beta Y + \gamma Z$$

Where the coefficients are real and $\alpha^2 + \beta^2 + \gamma^2 = 1$,

We first reason that since $O = O^\dagger$, O is of the form

$$O = \begin{pmatrix} x & y + zi \\ y - zi & w \end{pmatrix}$$

Where x, y, z, w are real. If we take

$$y = \alpha$$

$$z = -\beta$$

$$\frac{x - w}{2} = \gamma$$

$$\frac{x + w}{2} = \delta$$

We get

$$O = \begin{pmatrix} \delta + \gamma & \alpha - \beta i \\ \alpha + \beta i & \delta - \gamma \end{pmatrix} = \alpha X + \beta Y + \gamma Z + \delta \mathbb{I}$$

So any unitary O must be of this form. Since we also know that $O^2 = \mathbb{I}$, we have

$$O^2 = (\alpha X + \beta Y + \gamma Z + \delta \mathbb{I})(\alpha X + \beta Y + \gamma Z + \delta \mathbb{I})$$

And since $XY = -YX$, $XZ = -ZX$ and $YZ = -ZY$, if we expand and cancel, we get

$$O^2 = \alpha^2 X^2 + \beta^2 Y^2 + \gamma^2 Z^2 + \delta^2 \mathbb{I}^2 + 2\alpha\delta X + 2\beta\delta Y + 2\gamma\delta Z$$

$$O^2 = \alpha^2 \mathbb{I} + \beta^2 \mathbb{I} + \gamma^2 \mathbb{I} + \delta^2 \mathbb{I} + 2\alpha\delta X + 2\beta\delta Y + 2\gamma\delta Z$$

$$O^2 = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)\mathbb{I} + 2\alpha\delta X + 2\beta\delta Y + 2\gamma\delta Z$$

And so if this equals I, either $\delta = 0$ or $\alpha = \beta = \gamma = 0$. Since we are assuming nondegeneracy, the former is the case

$$O^2 = (\alpha^2 + \beta^2 + \gamma^2)\mathbb{I}$$

And so $\alpha^2 + \beta^2 + \gamma^2 = 1$. Thus, any single qubit observable can be represented in in this form.

(b) Referring to the result of Homework set 5, Problem 3(c), we found that the probability of success in the CHSH game was

$$p_s = \frac{1}{2} + \frac{1}{8}(\langle u_0|v_0\rangle + \langle u_0|v_1\rangle + \langle u_1|v_0\rangle - \langle u_1|v_1\rangle)$$

Where

$$\rangle u_x = A_x \otimes \mathbb{I}\rangle\psi$$
$$\rangle v_y = \mathbb{I} \otimes B_y\rangle\psi$$

From these definitions, we see

$$\begin{aligned}\langle u_x|v_y\rangle &= \langle\psi(A_x \otimes \mathbb{I}_B)(\mathbb{I}_A \otimes B_y)\rangle\psi \\ &= \langle\psi(A_x \otimes B_y)\rangle\psi\end{aligned}$$

And so we can rewrite the result of that problem as

$$p_s = \frac{1}{2} + \frac{1}{8}(\langle\psi(A_0 \otimes B_0)\rangle\psi + \langle\psi(A_0 \otimes B_1)\rangle\psi + \langle\psi(A_1 \otimes B_0)\rangle\psi - \langle\psi(A_1 \otimes B_1)\rangle\psi)$$

And by linearity

$$p_s = \frac{1}{2} + \frac{1}{8}(\langle\psi\mathcal{B}\rangle\psi)$$

Which is the correct identity.

(d) We have

$$\mathcal{B} = (A_0 \otimes B_0) + (A_0 \otimes B_1) + (A_1 \otimes B_0) - (A_1 \otimes B_1)$$

And from the special form of A_x, B_y, we have

$$A_x \otimes B_y = (\cos(\alpha_x)X + \sin(\alpha_x)Y) \otimes (\cos(\beta_y)X + \sin(\beta_y)Y)$$

And so we note that $ZXZ = -iZY = -X$ and $ZYZ = iZX = -Y$, and we see

$$(Z \otimes \mathbb{I})A_x \otimes B_y(Z \otimes \mathbb{I}) = (-\cos(\alpha_x)X - \sin(\alpha_x)Y) \otimes (\cos(\beta_y)X + \sin(\beta_y)Y) = -A_x \otimes B_y$$

And

$$(\mathbb{I} \otimes Z)A_x \otimes B_y(\mathbb{I} \otimes Z) = (\cos(\alpha_x)X + \sin(\alpha_x)Y) \otimes (-\cos(\beta_y)X - \sin(\beta_y)Y) = -A_x \otimes B_y$$

And so, since $\mathcal{B}$ is a linear combination of $A_x \otimes B_y$, we have by linearity

$$(Z \otimes \mathbb{I})\mathcal{B}(Z \otimes \mathbb{I}) = (\mathbb{I} \otimes Z)\mathcal{B}(\mathbb{I} \otimes Z) = -\mathcal{B}$$

Problem 6: Trading success probability for randomness in the CHSH game

Solution: (Due to De Huang)

(a) Let $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$, then

$$\rho_A = \mathbf{Tr}_B(\rho_{AB}) = \cos^2(\theta)|0\rangle\langle 0| + \sin^2(\theta)|1\rangle\langle 1|.$$

Assume that

$$A_x = |u_0^x\rangle\langle u_0^x| - |u_1^x\rangle\langle u_1^x|, \quad x \in \{0,1\},$$

where $\{|u_0^x\rangle, |u_1^x\rangle\}$ is an orthogonal basis. Then for any $a \in \{0,1\}$, $x \in \{0,1\}$, we have

$$\begin{aligned} p_\theta(a|x) &= \mathbf{Tr}(|u_a^x\rangle\langle u_a^x|\rho_A) \\ &= \cos^2(\theta)|\langle u_a^x|0\rangle|^2 + \sin^2(\theta)|\langle u_a^x|1\rangle|^2 \\ &\le \cos^2(\theta)|\langle u_a^x|0\rangle|^2 + \cos^2(\theta)|\langle u_a^x|1\rangle|^2 \\ &= \cos^2(\theta)\big(|\langle u_a^x|0\rangle|^2 + |\langle u_a^x|1\rangle|^2\big) \\ &= \cos^2(\theta). \end{aligned}$$

We have used the fact that $\sin^2(\theta) \le \cos^2(\theta),\ \forall\theta \in [0, \frac{\pi}{4}]$. Therefore $\max_{a,x} p_\theta(a|x) \le \cos^2(\theta)$.

(b) Using the result in problem 5(g), we have

$$I = 8p_s - 4 \le 8\big(\frac{1}{2} + \frac{1}{4}\sqrt{1+\sin^2(2\theta)}\big) - 4 = 2\sqrt{1+\sin^2(2\theta)}.$$

Since we may also assume that $p_s \ge \frac{1}{2}$, i.e. $I \ge 0$, then we have

$$\sin^2(2\theta) + 1 \ge \frac{I^2}{4},$$

$$\implies \quad 2 - \frac{I^2}{4} \ge 2 - (1+\sin^2(2\theta)) = 1 - \sin^2(2\theta) = \cos^2(2\theta),$$

$$\implies \quad \sqrt{2 - \frac{I^2}{4}} \ge \cos(2\theta) = 2\cos^2(\theta) - 1.$$

Then using the result of (a), we have

$$\max_{a,x}\ p_\theta(a|x) = \cos^2(\theta) \le \frac{1}{2}\big(1 + \sqrt{2 - \frac{I^2}{4}}\big),$$

i.e.

$$p_\theta(a|x) \le \frac{1}{2}\big(1 + \sqrt{2 - \frac{I^2}{4}}\big), \quad \forall a, x \in \{0,1\}.$$

(c) For any two-qubit $|\phi\rangle$, consider its Schmidt decomposition

$$|\phi\rangle = \cos(\theta)|u_0\rangle|v_0\rangle + \sin(\theta)|u_1\rangle|v_1\rangle,$$

where $\theta \in [0, \frac{\pi}{4}]$. We may also assume that

$$|u_0\rangle = U|0\rangle, \quad |u_1\rangle = U|1\rangle, \quad |v_0\rangle = V|0\rangle, \quad |v_1\rangle = V|1\rangle,$$

where U, V are two unitaries, that is

$$|\phi\rangle = \cos(\theta)(U|0\rangle \otimes V|0\rangle) + \sin(\theta)(U|1\rangle \otimes V|1\rangle) = (U \otimes V)|\psi_\theta\rangle.$$

Now assume that we use a strategy A_0, A_1, B_0, B_1 to play CHSH game with state $|\phi\rangle$, and have a probability distribution $\{p(a, b|x, y),\ a, b, x, y \in \{0, 1\}\}$. Let

$$\widetilde{A}_x = U^\dagger A_x U, \quad x \in \{0, 1\},$$

$$\widetilde{B}_y = U^\dagger B_y U, \quad y \in \{0, 1\}.$$

It's easy to check that $\widetilde{A}_0, \widetilde{A}_1, \widetilde{B}_0, \widetilde{B}_1$ are still non-degenerate observables. Then we can check that

$$\begin{aligned} p(a, b|x, y) &= \langle\phi|(A_x \otimes B_y)|\phi\rangle \\ &= \langle\psi_\theta|(U^\dagger \otimes V^\dagger)(A_x \otimes B_y)(U \otimes V)|\psi_\theta\rangle \\ &= \langle\psi_\theta|(\widetilde{A}_x \otimes \widetilde{B}_y)|\psi_\theta\rangle \\ &= \tilde{p}_\theta(a, b|x, y), \end{aligned}$$

where $\{\tilde{p}_\theta(a, b|x, y),\ a, b, x, y \in \{0, 1\}\}$ is the probability distribution when we use the observables $\widetilde{A}_0, \widetilde{A}_1, \widetilde{B}_0, \widetilde{B}_1$ to play CHSH game with the state $|\psi_\theta\rangle$. In partitcular, we have

$$p_s = \tilde{p}_s = \frac{1}{2} + \frac{1}{8} I,$$

$$p(a|x) = \tilde{p}_\theta(a|x) \leq \frac{1}{2}\big(1 + \sqrt{2 - \frac{I^2}{4}}\big), \quad \forall a, x \in \{0, 1\},$$

where we have used the result of (b). That is

$$p(a|x) \leq \frac{1}{2}\big(1 + \sqrt{2 - \frac{I^2}{4}}\big) = \frac{1}{2}\big(1 + \sqrt{2 - 4(2p_s - 1)^2}\big), \quad \forall a, x \in \{0, 1\}.$$

Then for any $x \in \{0, 1\}$,

$$\begin{aligned} H_{min}(A|X = x) = &\ -\log\big(\max_{a \in \{0,1\}} p(a|x)\big) \\ \geq &\ -\log\big(\frac{1}{2}\big(1 + \sqrt{2 - 4(2p_s - 1)^2}\big)\big) \\ = &\ 1 - \log\big(1 + \sqrt{2 - 4(2p_s - 1)^2}\big). \end{aligned}$$

(d) Let

$$A_0 = Z, \quad A_1 = X, \quad B_0 = \cos(t)Z + \sin(t)X, \quad B_1 = \cos(t)Z - \sin(t)X,$$

where $\cos(t) = \frac{1}{\sqrt{1+\sin^2(2\theta)}}$, $\sin(t) = \frac{\sin(2\theta)}{\sqrt{1+\sin^2(2\theta)}}$. It's easy to check that A_0, A_1, B_0, B_1 are non-degenerate observables. Then we have

$$\begin{aligned}\mathcal{B} &= A_0 \otimes B_0 + A_1 \otimes B_0 + A_0 \otimes B_1 - A_1 \otimes B_1 \\ &= 2\cos(t) Z \otimes Z + 2\sin(t) X \otimes X,\end{aligned}$$

and

$$\begin{aligned}\langle\psi_\theta|\mathcal{B}|\psi_\theta\rangle &= 2\cos(t)\langle\psi_\theta|Z\otimes Z|\psi_\theta\rangle + 2\sin(t)\langle\psi_\theta|X\otimes X|\psi_\theta\rangle \\ &= 2\cos(t) + 2\sin(t)\sin(2\theta) \\ &= 2\frac{1}{\sqrt{1+\sin^2(2\theta)}} + 2\frac{\sin^2(2\theta)}{\sqrt{1+\sin^2(2\theta)}} \\ &= 2\sqrt{1+\sin^2(2\theta)}.\end{aligned}$$

Recall that $p_s = \frac{1}{2} + \frac{1}{8}\langle\psi_\theta|\mathcal{B}|\psi_\theta\rangle = \frac{1}{2} + \frac{1}{8}I$, thus

$$I = \langle\psi_\theta|\mathcal{B}|\psi_\theta\rangle = 2\sqrt{1+\sin^2(2\theta)},$$

$$\frac{1}{2}\big(1+\sqrt{2-\frac{I^2}{4}}\big) = \frac{1}{2}\big(1+\sqrt{1-\sin^2(2\theta)}\big) = \frac{1}{2}(1+\cos(2\theta)) = \cos^2(\theta).$$

On the other hand, since $\forall x \in \{0,1\}$,

$$p(0|x) - p(1|x) = \mathbf{Tr}(A_x\rho_A), \quad p(0|x) + p(1|x) = 1,$$

we have

$$p(0|x) = \frac{1}{2}\big(1+\mathbf{Tr}(A_x\rho_A)\big), \quad p(1|x) = \frac{1}{2}\big(1-\mathbf{Tr}(A_x\rho_A)\big).$$

Then now we have

$$\rho_A = \cos^2(\theta)|0\rangle\langle 0| + \sin^2(\theta)|1\rangle\langle 1|,$$

$$p(0|0) = \frac{1}{2}\big(1+\mathbf{Tr}(A_0\rho_A)\big) = \frac{1}{2}\big(1+\cos^2(\theta)-\sin^2(\theta)\big) = \cos^2(\theta),$$

$$p(1|0) = \frac{1}{2}\big(1-\mathbf{Tr}(A_0\rho_A)\big) = \frac{1}{2}\big(1-\cos^2(\theta)+\sin^2(\theta)\big) = \sin^2(\theta),$$

$$p(0|1) = \frac{1}{2}\big(1+\mathbf{Tr}(A_1\rho_A)\big) = \frac{1}{2},$$

$$p(1|1) = \frac{1}{2}\big(1-\mathbf{Tr}(A_1\rho_A)\big) = \frac{1}{2}.$$

Since $\theta \in [0, \frac{\pi}{4}]$, we have $\cos^2(\theta) \geq \frac{1}{2} \geq \sin^2(\theta)$, thus

$$\max_{a,x}\ p(a|x) = \cos^2(\theta) = \frac{1}{2}\big(1+\sqrt{2-\frac{I^2}{4}}\big).$$

The bound is tight.