CS/Ph120 Homework 5 Solutions

November 11, 2016

Problem 1: A dual formulation for the conditional min-entropy

Solution: (Due to De Huang)

(a) For any $|\Psi\rangle_{XE} \in \mathcal{H}_X \otimes \mathcal{H}_E$, say

$$|\Psi\rangle_{XE} = \sum_{i,j} \alpha_{i,j} |i\rangle_X |j\rangle_E,$$

we have

$$\begin{aligned}
\langle\Psi|_{XE}(|x\rangle\langle x| \otimes N_x)|\Psi\rangle_{XE} &= \sum_{i,j}\sum_{k,l} \langle i|_X \langle j|_E (|x\rangle\langle x| \otimes N_x)|k\rangle_X |l\rangle_E \\
&= \sum_{i,j}\sum_{k,l} \langle i|x\rangle\langle x|k\rangle_X \langle j|N_x|l\rangle_E \\
&= \big(\sum_{i,k} \langle i|x\rangle\langle x|k\rangle_X\big)\big(\sum_{j,l} \langle j|N_x|l\rangle_E\big) \\
&= \Big(\big(\sum_i \langle i|_X\big)|x\rangle\langle x|\big(\sum_i |i\rangle_X\big)\Big)\Big(\big(\sum_j \langle j|_E\big)N_x\big(\sum_j |j\rangle_E\big)\Big) \\
&\geq 0.
\end{aligned}$$

Thus $|x\rangle\langle x| \otimes N_x \geq 0,\ \forall x \in \mathcal{X}$, and consequently

$$Z = \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes N_x \geq 0.$$

By definition we have

$$\begin{aligned}\Phi(Z) &= \sum_{x'\in\mathcal{X}} (\langle x'| \otimes \mathbb{I}_E) Z (|x'\rangle \otimes \mathbb{I}_E) \\ &= \sum_{x,x'\in\mathcal{X}} (\langle x'| \otimes \mathbb{I}_E)(|x\rangle\langle x| \otimes N_x)(|x'\rangle \otimes \mathbb{I}_E) \\ &= \sum_{x,x'\in\mathcal{X}} \langle x'|x\rangle\langle x|x'\rangle N_x \\ &= \sum_{x\in\mathcal{X}} N_x \\ &= \mathbb{I}_E.\end{aligned}$$

(b)

$$\begin{aligned}tr(Z\rho_{XE}) &= tr\big(\sum_{x,x'\in\mathcal{X}} (|x\rangle\langle x|x'\rangle\langle x'|) \otimes (N_x \rho_{x'}^E)\big) \\ &= \sum_{x,x'\in\mathcal{X}} tr\big(|x\rangle\langle x|x'\rangle\langle x'|\big) tr\big(N_x\rho_{x'}^E\big) \\ &= \sum_{x\in\mathcal{X}} tr\big(N_x\rho_x^E\big)\end{aligned}$$

(c) For any $|\phi\rangle_E \in \mathcal{H}_E$, we have

$$\langle\phi|_E N_x |\phi\rangle_E = \langle\phi|_E (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E) |\phi\rangle_E = (\langle x| \otimes \langle\phi|_E) Z (|x\rangle \otimes |\phi\rangle_E) \geq 0,$$

thus $N_x \geq 0,\ \forall x \in \mathcal{X}$. Also we have

$$\sum_{x\in\mathcal{X}} N_x = \sum_{x\in\mathcal{X}} (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E) = \Phi(Z) = \mathbb{I}_E.$$

Therefore $\{N_x\}_x$ is a valid POVM over $\mathcal{H}_E$.

(d) By the previous resluts, the constraint that $\{M_x\}_x$ is a POVM can be translated into the conditions

$$M_x = (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E), \quad \forall x \in \mathcal{X},$$

for some Z satisfying

$$Z \geq 0, \quad \Phi(Z) = \mathbb{I}_E,$$

where

$$\Phi(Z) = \sum_{x\in\mathcal{X}} (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E).$$

And the objective function can rewrite as

$$\sum_{x\in\mathcal{X}} tr\big(M_x\rho_x^E\big) = tr(Z\rho_{XE}).$$

Therefore the primal problem that gives P_{guess} is

$$\begin{aligned} P_{guess}(X|E) = \sup_{Z} \ & tr(Z\rho_{XE}) \\ s.t. \quad & \Phi(Z) = \mathbb{I}_E, \\ & Z \geq 0. \end{aligned}$$

In the language of HW3 Problem 2, we are using $A = \rho_{XE}$, $B = \mathbb{I}_E$.

(e) Since

$$\Phi(Z) = \sum_{x\in\mathcal{X}} (\langle x| \otimes \mathbb{I}_E) Z (|x\rangle \otimes \mathbb{I}_E) \quad \forall Z,$$

we have

$$\begin{aligned} \Phi^*(Y_E) &= \sum_{x\in\mathcal{X}} (|x\rangle \otimes \mathbb{I}_E) Y_E (\langle x| \otimes \mathbb{I}_E) \\ &= \sum_{x\in\mathcal{X}} (|x\rangle\langle x| \otimes Y_E) \\ &= \big(\sum_{x\in\mathcal{X}} |x\rangle\langle x|\big) \otimes Y_E \\ &= \mathbb{I}_X \otimes Y_E, \quad \forall Y_E. \end{aligned}$$

(f) Recall that the dual problem is

$$\begin{aligned} \inf_{Y} \ & tr(BY) \\ s.t. \quad & \Phi^*(Y) \geq A, \\ & Y = Y^\dagger. \end{aligned}$$

Since we are using we are using $A = \rho_{XE}$, $B = \mathbb{I}_E$, thus the dual problem becomes

$$\begin{aligned} \inf_{Y} \ & tr(Y) \\ s.t. \quad & \mathbb{I}_X \otimes Y \geq \rho_{XE}, \\ & Y = Y^\dagger. \end{aligned}$$

Moreover, if $\mathbb{I}_X \otimes Y \geq \rho_{XE}$, given any $|\phi\rangle_E \in \mathcal{H}_E$, we have

$$\begin{aligned} \langle\phi|_E (Y - \rho_x^E) |\phi\rangle_E &= \langle\phi|_E Y |\phi\rangle_E - \langle\phi|_E \rho_x^E |\phi\rangle_E \\ &= (\langle x|\langle\phi|_E)(\mathbb{I}_X \otimes Y)(|x\rangle|\phi\rangle_E) - (\langle x|\langle\phi|_E)(\sum_{x'\in\mathcal{X}} |x'\rangle\langle x'| \otimes \rho_{x'}^E)(|x\rangle|\phi\rangle_E) \\ &= (\langle x|\langle\phi|_E)(\mathbb{I}_X \otimes Y)(|x\rangle|\phi\rangle_E) - (\langle x|\langle\phi|_E)\rho_X E(|x\rangle|\phi\rangle_E) \\ &= (\langle x|\langle\phi|_E)(\mathbb{I}_X \otimes Y - \rho_{XE})(|x\rangle|\phi\rangle_E) \\ &\geq 0, \end{aligned}$$

thus $Y \geq \rho_x^E, \ \forall x \in \mathcal{X}$. Conversely, if $Y \geq \rho_x^E, \ \forall x \in \mathcal{X}$, then

$$\mathbb{I}_X \otimes Y = \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes Y \geq \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_x^E = \rho_{XE}.$$

Therefore we have

$$\mathbb{I}_X \otimes Y \geq \rho_{XE} \quad \Longleftrightarrow \quad Y \geq \rho_x^E,\ \forall x \in \mathcal{X},$$

the dual problem is more explicitly as

$$\begin{aligned} &\inf_Y \ tr(Y) \\ s.t. \quad &Y \geq \rho_x,\ \forall x \in \mathcal{X}, \\ &Y = Y^\dagger. \end{aligned}$$

(g) Since the primal SDP problem is strictly feasible and the objective function is bounded above by 1, the problem has strong duality. That is, the supremum of the primal probelm and the infimum of the dual problem are the same, i.e. we have

$$\begin{aligned} P_{guess}(X|E) = &\inf_Y \ tr(Y) \\ s.t. \quad &Y \geq \rho_x,\ \forall x \in \mathcal{X}, \\ &Y = Y^\dagger, \end{aligned}$$

which is what we want to conclude.

(h) Given that $\sigma \geq \rho_x,\ \forall x \in \mathcal{X}$, we have

$$P_{guess}(X|E) = \sup_{M_x} \sum_{x\in\mathcal{X}} tr(M_x\rho_x) \leq \sup_{M_x} \sum_{x\in\mathcal{X}} tr(M_x\sigma) = \sup_{M_x} tr\big((\sum_{x\in\mathcal{X}} M_x)\sigma\big) = tr(\mathbb{I}_E\sigma) = tr(\sigma).$$

(i) Suppose that

$$\tau_{X_1E_1} = \sum_{x\in\mathcal{X}_1} |x\rangle\langle x| \otimes \tau_x^{E_1},$$

then

$$\begin{aligned} \rho_{XE} &= \tau_{X_1E_1}^{\otimes n} \\ &= \sum_{x_1,x_2,\ldots,x_n\in\mathcal{X}_1} \big((|x_1\rangle\langle x_1| \otimes \tau_{x_1}^{E_1}) \otimes (|x_2\rangle\langle x_2| \otimes \tau_{x_2}^{E_1}) \otimes \cdots \otimes (|x_n\rangle\langle x_n| \otimes \tau_{x_n}^{E_1})\big) \\ &= \sum_{x_1,x_2,\ldots,x_n\in\mathcal{X}_1} \big(|x_1x_2\ldots x_n\rangle\langle x_1x_2\ldots x_n|\big) \otimes \big(\tau_{x_1}^{E_1} \otimes \tau_{x_2}^{E_1} \otimes \cdots \otimes \tau_{x_n}^{E_1}\big) \\ &= \sum_{\boldsymbol{x}\in\mathcal{X}} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes \rho_{\boldsymbol{x}}^E, \end{aligned}$$

where

$$\begin{aligned} \mathcal{X} &= \{\boldsymbol{x} = (x_1, x_2, \ldots, x_n) : x_i \in \mathcal{X}_1,\ i = 1, 2, \ldots, n\}, \\ \rho_{\boldsymbol{x}}^E &= \tau_{x_1}^{E_1} \otimes \tau_{x_2}^{E_1} \otimes \cdots \otimes \tau_{x_n}^{E_1}, \quad \forall x \in \mathcal{X}. \end{aligned}$$

Using the previous results, we have

$$P_{guess}(X_1|E_1) = \sup_{\{M_x\}\in P_1} \sum_{x\in\mathcal{X}_1} tr(M_x\tau_x^{E_1}) = \inf_{\sigma\in\Omega_1} \ tr(\sigma),$$

$$P_{guess}(X|E) = \sup_{\{\boldsymbol{M_x}\}\in P} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(\boldsymbol{M_x}\rho_{\boldsymbol{x}}^E) = \inf_{\boldsymbol{\sigma}\in\Omega}\ tr(\boldsymbol{\sigma}),$$

where

$$P_1 = \{\{M_x^1\} : \{M_x^1\} \text{ is a POVM over } \mathcal{H}_{E_1}\},$$
$$\Omega_1 = \{\sigma : \sigma \geq \tau_x^{E_1},\ \forall x \in \mathcal{X}_1\},$$
$$P = \{\{\boldsymbol{M_x}\} :\ \{\boldsymbol{M_x}\} \text{ is a POVM over } \mathcal{H}_E\},$$
$$\Omega = \{\boldsymbol{\sigma} :\ \boldsymbol{\sigma} \geq \rho_{\boldsymbol{x}}^E,\ \forall \boldsymbol{x} \in \mathcal{X}\}.$$

Define

$$\widetilde{P} = \{\{\boldsymbol{M_x}\} = \{M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n}\}_{\boldsymbol{x}} :\ \{M_{x_i}\} \in P_1,\ i = 1, 2, \ldots, n\},$$

$$\widetilde{\Omega} = \{\boldsymbol{\sigma} = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n :\ \sigma_i \in \Omega_1,\ i = 1, 2, \ldots, n\},$$

then it's easy to check that

$$\widetilde{P} \subset P, \quad \widetilde{\Omega} \subset \Omega,$$

and thus we have

$$P_{guess}(X|E) = \sup_{\{\boldsymbol{M_x}\}\in P} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(\boldsymbol{M_x}\rho_{\boldsymbol{x}}^E) \geq \sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(\boldsymbol{M_x}\rho_{\boldsymbol{x}}^E),$$

$$P_{guess}(X|E) = \inf_{\boldsymbol{\sigma}\in\Omega}\ tr(\boldsymbol{\sigma}) \leq \inf_{\boldsymbol{\sigma}\in\widetilde{\Omega}}\ tr(\boldsymbol{\sigma}).$$

But on the other hand, we have

$$\begin{aligned}
\sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(M_{\boldsymbol{x}}\rho_{\boldsymbol{x}}^E) &= \sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \sum_{\boldsymbol{x}\in\mathcal{X}} tr\big((M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n})(\tau_{x_1}^{E_1} \otimes \tau_{x_2}^{E_1} \otimes \cdots \otimes \tau_{x_n}^{E_1})\big) \\
&= \sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \sum_{\boldsymbol{x}\in\mathcal{X}} \big(\prod_{i=1}^n tr(M_{x_i}\tau_{x_i}^{E_1})\big) \\
&= \sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \prod_{i=1}^n \big(\sum_{x_i\in\mathcal{X}_1} tr(M_{x_i}\tau_{x_i}^{E_1})\big) \\
&= \prod_{i=1}^n \big(\sup_{\{M_{x_i}\}\in P_1} \sum_{x_i\in\mathcal{X}_1} tr(M_{x_i}\tau_{x_i}^{E_1})\big) \\
&= \big(P_{guess}(X_1|E_1)\big)^n,
\end{aligned}$$

$$\begin{aligned}
\inf_{\boldsymbol{\sigma}\in\widetilde{\Omega}}\ tr(\boldsymbol{\sigma}) &= \inf_{\boldsymbol{\sigma}\in\widetilde{\Omega}}\ tr(\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n) \\
&= \inf_{\boldsymbol{\sigma}\in\widetilde{\Omega}} \prod_{i=1}^n tr(\sigma_i) \\
&= \prod_{i=1}^n \big(\inf_{\sigma_i\in\Omega_1}\ tr(\sigma_i)\big) \\
&= \big(P_{guess}(X_1|E_1)\big)^n.
\end{aligned}$$

Thus we come to

$$P_{guess}(X|E) = \sup_{\{\boldsymbol{M_x}\}\in P} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(\boldsymbol{M_x}\rho_{\boldsymbol{x}}^E) \geq \sup_{\{\boldsymbol{M_x}\}\in \widetilde{P}} \sum_{\boldsymbol{x}\in\mathcal{X}} tr(\boldsymbol{M_x}\rho_{\boldsymbol{x}}^E) = \big(P_{guess}(X_1|E_1)\big)^n,$$

$$P_{guess}(X|E) = \inf_{\boldsymbol{\sigma}\in\Omega} tr(\boldsymbol{\sigma}) \leq \inf_{\boldsymbol{\sigma}\in\widetilde{\Omega}} tr(\boldsymbol{\sigma}) = \big(P_{guess}(X_1|E_1)\big)^n,$$

$$\implies \quad P_{guess}(X|E) \geq \big(P_{guess}(X_1|E_1)\big)^n \geq P_{guess}(X|E),$$

$$\implies \quad P_{guess}(X|E) = \big(P_{guess}(X_1|E_1)\big)^n,$$

and therefore

$$\begin{aligned} H_{min}(X|E)_\rho &= -\log P_{guess}(X|E) \\ &= -\log\big(P_{guess}(X_1|E_1)\big)^n \\ &= -n\log P_{guess}(X_1|E_1) \\ &= nH_{min}(X_1|E_1)_\tau. \end{aligned}$$

Problem 2: Computing the min-entropy

Solution: (Due to Mandy Huo)

(a) By definition $H_{\min}(X \mid E) = -\log P_{\text{guess}}(X \mid E)$ and $H_{\min}(X) = -\log \max_x p_x = -\log P_{\text{guess}}(X)$ so we want to show $-\log P_{\text{guess}}(X \mid E) \geq -\log P_{\text{guess}}(X) - \log|E| = -\log(P_{\text{guess}}(X)|E|)$. Since $-\log x$ is monotonically decreasing, we need to show $P_{\text{guess}}(X \mid E) \leq P_{\text{guess}}(X)|E|$.

(b) Let $A \geq 0$, $B \geq 0$. We write the eigendecomposition $B = \sum_i \lambda_i(B)|u_i\rangle\langle u_i|$. Then using the linearity of trace we have

$$\begin{aligned} \mathbf{Tr}\,(AB) = \mathbf{Tr}\left(A\sum_i \lambda_i(B)|u_i\rangle\langle v_i|\right) &= \sum_i \lambda_i(B)\mathbf{Tr}\,(A|u_i\rangle\langle u_i|) \\ &\leq \lambda_{\max}(B)\sum_i \mathbf{Tr}\,(A|u_i\rangle\langle u_i|) \\ &= \lambda_{\max}(B)\mathbf{Tr}\left(A\sum_i |u_i\rangle\langle u_i|\right) \\ &= \lambda_{\max}(B)\mathbf{Tr}\,(A\cdot\mathbb{I}) \\ &= \lambda_{\max}(B)\mathbf{Tr}\,(A) \end{aligned}$$

where the inequality step is because $\mathbf{Tr}\,(A|u_i\rangle\langle u_i|) = \langle u_i|A|u_i\rangle \geq 0$ since $A \geq 0$.

(c) Let $\{M_x\}$ be a POVM and ρ_x^E be a quantum state. Then $M_x \geq 0$ and since ρ_x^E is a density matrix, we have $\rho_x^E \geq 0$ so $\lambda_i(\rho_x^E) \geq 0$ so $\sum_i \lambda_i(\rho_x^E) = \mathbf{Tr}\left(\rho_x^E\right) = 1 \Rightarrow \lambda_{\max}(\rho_x^E) \leq 1$. Then applying part (b) gives

$$\mathbf{Tr}\left(M_x\rho_x^E\right) \leq \lambda_{\max}(\rho_x^E)\mathbf{Tr}\,(M_x) \leq \mathbf{Tr}\,(M_x)\,.$$

(d) Since $p_x \geq 0$, applying part (c),

$$\begin{aligned}\sum_x p_x \mathbf{Tr}\left(M_x \rho_x^E\right) \leq \sum_x p_x \mathbf{Tr}\left(M_x\right) &\leq \left(\max_x p_x\right) \sum_x \mathbf{Tr}\left(M_x\right) \\ &= \left(\max_x p_x\right) \mathbf{Tr}\left(\sum_x M_x\right) \\ &= \left(\max_x p_x\right) \mathbf{Tr}\left(\mathbb{I}_E\right) \\ &= \left(\max_x p_x\right) |E|.\end{aligned}$$

Then we have

$$P_{\text{guess}}(X \mid E) = \max_{\{M_x\}_x} \sum_x p_x \mathbf{Tr}\left(M_x \rho_x^E\right) \leq \left(\max_x p_x\right) |E|.$$

Since $-\log x$ is monotonically decreasing, we have

$$\begin{aligned}H_{\min}(X \mid E) = -\log P_{\text{guess}}(X \mid E) \geq -\log\left(\left(\max_x p_x\right)|E|\right) &= -\log\left(\max_x p_x\right) - \log|E| \\ &= H_{\min}(X) - \log|E|.\end{aligned}$$

Problem 3: Bounding the winning probability in the CHSH game

Solution: (Due to De Huang)

(a) Since $\{A_x^0, A_x^1\}$ is a valid POVM, we have

$$\begin{aligned}&0 \leq A_x^0 \leq \mathbb{I}_A, \quad 0 \leq A_x^1 \leq \mathbb{I}_A, \\ \Longrightarrow \quad &-\mathbb{I}_A \leq A_x = A_x^0 - A_x^1 \leq \mathbb{I}_A, \\ \Longrightarrow \quad &r(A_x) \leq 1,\end{aligned}$$

where $r(A_x)$ denotes the spectral radius of A_x. Since A_x^0, A_x^1 are Hermitian, A_x is also Hermitian, thus the largest singular value of A_x equals to $r(A_x)$. Therefore

$$\|A_x\| = r(A_x) \leq 1.$$

The same argument also work for B_y, i.e. $\|B_y\| \leq 1$.

(b) Suppose that A_x is diagonalized in a basis $\{|\phi_i\rangle\}$, i.e.

$$A_x|\phi_i\rangle = \lambda_i|\phi_i\rangle, \quad i = 0, 1, \ldots, d_a - 1,$$

$$\langle\phi_i|\phi_j\rangle = \delta_{i,j}, \quad i, j = 0, 1, \ldots, d_a - 1,$$

where d_a is the dimension of $\mathcal{H}_A$, and $\lambda_i,\ i = 0, 1, \ldots, d_a - 1$, are all eigencalues of A_x. Then

$$\lambda_i^2 \leq \|A_x\|^2 \leq 1, \quad i = 0, 1, \ldots, d_a - 1,$$

since A_x is Hermitian. We can always write $|\psi\rangle_{AB}$ as

$$|\psi\rangle_{AB} = \sum_{i=0}^{d_a-1}\sum_{j=0}^{d_b-1} \alpha_{i,j}|\phi_i\rangle_A|j\rangle_B.$$

Then we have

$$\begin{aligned}
\||u_x\rangle\|^2 &= \langle u_x|u_x\rangle \\
&= \langle\psi|_{AB}(A_x\otimes\mathbb{I}_B)(A_x\otimes\mathbb{I}_B)|\psi\rangle_{AB} \\
&= \sum_{i,j}\sum_{k,l}\overline{\alpha_{i,j}}\alpha_{k,l}\langle\psi_i|A_x^2|\psi_k\rangle_A\langle j|l\rangle_B \\
&= \sum_{i,j}\sum_{k,l}\overline{\alpha_{i,j}}\alpha_{k,l}\lambda_i\lambda_k\langle\psi_i|\psi_k\rangle_A\langle j|l\rangle_B \\
&= \sum_{i,j}|\alpha_{i,j}|^2\lambda_i^2 \\
&\le \sum_{i,j}|\alpha_{i,j}|^2 \\
&= \||\psi\rangle_{AB}\|^2 \\
&= 1,
\end{aligned}$$

that is $\||u_x\rangle\| \le 1$. Similarly we can also prove that $\||v_y\rangle\| \le 1$.

(c) By direct calculation, we have

$$\begin{aligned}
\langle u_x|v_y\rangle &= \langle\psi|_{AB}(A_x\otimes\mathbb{I}_B)(\mathbb{I}_A\otimes B_y)|\psi\rangle_{AB} \\
&= \langle\psi|_{AB}(A_x\otimes B_y)|\psi\rangle_{AB} \\
&= \langle\psi|_{AB}(A_x^0\otimes B_y^0)|\psi\rangle_{AB} - \langle\psi|_{AB}(A_x^1\otimes B_y^0)|\psi\rangle_{AB} \\
&\quad - \langle\psi|_{AB}(A_x^0\otimes B_y^1)|\psi\rangle_{AB} + \langle\psi|_{AB}(A_x^1\otimes B_y^1)|\psi\rangle_{AB}.
\end{aligned}$$

Then for $(x,y)\neq(1,1)$,

$$\begin{aligned}
\langle u_x|v_y\rangle &= 2\langle\psi|_{AB}(A_x^0\otimes B_y^0)|\psi\rangle_{AB} + 2\langle\psi|_{AB}(A_x^1\otimes B_y^1)|\psi\rangle_{AB} \\
&\quad - \langle\psi|_{AB}(A_x^0\otimes B_y^0)|\psi\rangle_{AB} - \langle\psi|_{AB}(A_x^1\otimes B_y^0)|\psi\rangle_{AB} \\
&\quad - \langle\psi|_{AB}(A_x^0\otimes B_y^1)|\psi\rangle_{AB} - \langle\psi|_{AB}(A_x^1\otimes B_y^1)|\psi\rangle_{AB} \\
&= 2\mathbf{Tr}\big((A_x^0\otimes B_y^0)|\psi\rangle\langle\psi|_{AB}\big) + 2\mathbf{Tr}\big((A_x^1\otimes B_y^1)|\psi\rangle\langle\psi|_{AB}\big) \\
&\quad - \langle\psi|_{AB}\big((A_x^0+A_x^1)\otimes(B_y^0+B_y^1)\big)|\psi\rangle_{AB} \\
&= 2p(0,0|x,y) + 2p(1,1|x,y) - \langle\psi|_{AB}(\mathbb{I}_A\otimes\mathbb{I}_B)|\psi\rangle_{AB} \\
&= 2p(0,0|x,y) + 2p(1,1|x,y) - 1,
\end{aligned}$$

$$p(0,0|x,y) + p(1,1|x,y) = \frac{1}{2}(1+\langle u_x|v_y\rangle),$$

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

$$\begin{aligned}\langle u_x|v_y\rangle &= \langle\psi|_{AB}(A_x^0\otimes B_y^0)|\psi\rangle_{AB}+\langle\psi|_{AB}(A_x^1\otimes B_y^0)|\psi\rangle_{AB}\\ &\quad+\langle\psi|_{AB}(A_x^0\otimes B_y^1)|\psi\rangle_{AB}+\langle\psi|_{AB}(A_x^1\otimes B_y^1)|\psi\rangle_{AB}\\ &\quad-2\langle\psi|_{AB}(A_x^1\otimes B_y^0)|\psi\rangle_{AB}-2\langle\psi|_{AB}(A_x^0\otimes B_y^1)|\psi\rangle_{AB}\\ &=\langle\psi|_{AB}\big((A_x^0+A_x^1)\otimes(B_y^0+B_y^1)\big)|\psi\rangle_{AB}\\ &\quad-2\mathbf{Tr}\big((A_x^1\otimes B_y^0)|\psi\rangle\langle\psi|_{AB}\big)-2\mathbf{Tr}\big((A_x^0\otimes B_y^1)|\psi\rangle\langle\psi|_{AB}\big)\\ &=\langle\psi|_{AB}(\mathbb{I}_A\otimes\mathbb{I}_B)|\psi\rangle_{AB}-2p(1,0|x,y)-2p(0,1|x,y)\\ &=1-2p(1,0|x,y)+2p(0,1|x,y),\end{aligned}$$

$$p(1,0|x,y)+p(0,1|x,y)=\frac{1}{2}(1-\langle u_x|v_y\rangle).$$

Finally we have

$$\begin{aligned}p_{succ} &= \sum_{x,y\in\{0,1\}}p(x,y)\sum_{a\oplus b=x\wedge y}p(a,b|x,y)\\ &=\frac{1}{4}\big(p(0,0|0,0)+p(1,1|0,0)+p(0,0|1,0)+p(1,1|1,0)\\ &\quad+p(0,0|0,1)+p(1,1|0,1)+p(1,0|1,1)+p(0,1|1,1)\big)\\ &=\frac{1}{8}\big(\langle u_0|v_0\rangle+1+\langle u_1|v_0\rangle+1+\langle u_0|v_1\rangle+1+1-\langle u_1|v_1\rangle\big)\\ &=\frac{1}{2}+\frac{1}{8}\big(\langle u_0|v_0\rangle+\langle u_1|v_0\rangle+\langle u_0|v_1\rangle-\langle u_1|v_1\rangle\big).\end{aligned}$$

(d) Let $c=\max\{\||r_0\rangle\|,\||r_1\rangle\|,\||s_0\rangle\|,\||s_1\rangle\|\}$. Notice that

$$\begin{aligned}\||r_0\rangle+|r_1\rangle\|^2+\||r_0\rangle-|r_1\rangle\|^2 &= (\langle r_0|+\langle r_1|)(|r_0\rangle+|r_1\rangle)+(\langle r_0|-\langle r_1|)(|r_0\rangle-|r_1\rangle)\\ &=2\langle r_0|r_0\rangle+2\langle r_0|r_0\rangle\\ &=2\||r_0\rangle\|^2+2\||r_1\rangle\|^2\\ &\le 4c^2,\end{aligned}$$

thus

$$\||r_0\rangle+|r_1\rangle\|+\||r_0\rangle-|r_1\rangle\|\le\sqrt{2}\Big(\||r_0\rangle+|r_1\rangle\|^2+\||r_0\rangle-|r_1\rangle\|^2\Big)^{\frac{1}{2}}\le 2\sqrt{2}c.$$

Then we have

$$\begin{aligned}\big|\langle r_0|s_0\rangle+\langle r_1|s_0\rangle+\langle r_0|s_1\rangle-\langle r_1|s_1\rangle\big| &\le \big|\langle r_0|s_0\rangle+\langle r_1|s_0\rangle\big|+\big|\langle r_0|s_1\rangle-\langle r_1|s_1\rangle\big|\\ &=\big|(\langle r_0|+\langle r_1|)|s_0\rangle\big|+\big|(\langle r_0|-\langle r_1|)|s_1\rangle\big|\\ &\le\||r_0\rangle+|r_1\rangle\|\||s_0\rangle\|+\||r_0\rangle-|r_1\rangle\|\||s_1\rangle\|\\ &\le c\||r_0\rangle+|r_1\rangle\|+c\||r_0\rangle-|r_1\rangle\|\\ &\le 2\sqrt{2}c^2.\end{aligned}$$

(e) Using the result of (b), we have

$$c = \max\{\||u_0\rangle\|, \||u_1\rangle\|, \||s_0\rangle\|, \||s_1\rangle\|\} \leq 1.$$

Then using the result of (d), we have

$$\big|\langle u_0|v_0\rangle + \langle u_1|v_0\rangle + \langle u_0|v_1\rangle - \langle u_1|v_1\rangle\big| \leq 2\sqrt{2}c^2 \leq 2\sqrt{2}.$$

Finally using the result of (c), we have

$$\begin{aligned} p_{succ} &= \frac{1}{2} + \frac{1}{8}\big(\langle u_0|v_0\rangle + \langle u_1|v_0\rangle + \langle u_0|v_1\rangle - \langle u_1|v_1\rangle\big) \\ &\leq \frac{1}{2} + \frac{1}{8}\big|\langle u_0|v_0\rangle + \langle u_1|v_0\rangle + \langle u_0|v_1\rangle - \langle u_1|v_1\rangle\big| \\ &\leq \frac{1}{2} + \frac{\sqrt{2}}{4} \\ &= \cos^2\frac{\pi}{8}. \end{aligned}$$

Problem 4: A guessing game

Solution: (Due to Mandy Huo, adapted by the TAs)

(a) If Eve knows both θ and U_A then she can guess perfectly in all cases by applying $U_E = \overline{U}_A$, the element-wise complex conjugation of U_A, and measuring in the same basis as Alice. This is because, from Homework 4, we know that $U \otimes \mathbb{I}|\phi^+\rangle = \mathbb{I} \otimes U^T|\phi^+\rangle$, and to undo U^T Eve just applies $(U^T)^\dagger = \overline{U}$.

(b) Alice should use the following strategy:

1. If $\theta = 0$ then Alice applies $\mathbb{I}$ with probability 1/2, X with probability 1/2, or Z with probability zero before measuring.
2. If $\theta = 1$ then Alice applies $\mathbb{I}$ with probability 1/2, Z with probability 1/2, or X with probability zero before measuring.

With this strategy, when $\theta = 0$, the shared state is either $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, each with probability 1/2. So if $x = 0$, since Eve does not know which unitary Alice applied, Eve has the state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, and if $x = 1$, Eve has the state $\frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|0\rangle\langle 0|$. Then Eve cannot distinguish between the two outcomes so at best she can guess randomly.

Similarly, when $\theta = 1$ the shared state is either $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ or $\frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$, each with probability 1/2. So if $x = 0$, Eve has the state $\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$, and if $x = 1$, Eve has the state $\frac{1}{2}|-\rangle\langle -| + \frac{1}{2}|+\rangle\langle +|$. Hence in both cases Eve's best strategy is to guess randomly so she will guess correctly with probability 1/2. Since the worst strategy Eve can use is a random guess, this strategy makes Eve's guessing probability the lowest possible.

(c) Alice should, for all θ, first apply either $\mathbb{I}$ or $Y = XZ$ each with probability 1/2. We will show that this achieves the same probability as in part (b).

With this strategy, when $\theta = 0$, the shared state is either $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ or $\frac{1}{\sqrt{2}}(-|01\rangle + |10\rangle)$, each with probability 1/2. Then if $x = 0$, since Eve does not know which unitary Alice used, Eve has the state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, and if $x = 1$, Eve has the state $\frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|0\rangle\langle 0|$. Then Eve cannot distinguish between the two so at best she can guess randomly.

Similarly, when $\theta = 1$ the shared state is either $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ or $\frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$, each with probability 1/2. So if $x = 0$, Eve has the state $\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$, and if $x = 1$, Eve has the state $\frac{1}{2}|-\rangle\langle -| + \frac{1}{2}|+\rangle\langle +|$. Hence in both cases Eve's best strategy is to guess randomly so she will guess correctly with probability 1/2.

Problem 5: Decoherence

Solution: (Due to Mandy Huo)

We have $|\Psi\rangle|E\rangle \mapsto \alpha|0\rangle|E_0\rangle + \beta|1\rangle|E_1\rangle$ so

$$\begin{aligned}|\Psi\rangle\langle\Psi| \otimes |E\rangle\langle E| = |\alpha|^2|0\rangle\langle 0| \otimes |E_0\rangle\langle E_0| + \alpha\beta^*|0\rangle\langle 1| \otimes |E_0\rangle\langle E_1| \\ + \alpha^*\beta|1\rangle\langle 0| \otimes |E_1\rangle\langle E_0| + |\beta|^2|1\rangle\langle 1| \otimes |E_1\rangle\langle E_1|.\end{aligned}$$

Assuming $\langle E_0|E_1\rangle$ is real, we have $\langle E_0|E_1\rangle = \langle E_1|E_0\rangle$. Since $|E\rangle$, $|E_0\rangle$, and $|E_1\rangle$ are normalized, tracing out the environment gives

$$|\Psi\rangle\langle\Psi| \otimes \mathbf{Tr}\left(|E\rangle\langle E|\right) = |\alpha|^2|0\rangle\langle 0| + \langle E_0|E_1\rangle(\alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0|) + |\beta|^2|1\rangle\langle 1|$$

Define $p = \frac{1-\langle E_0|E_1\rangle}{2}$. We will show later that p is in fact a valid probability. Note that $Z|\Psi\rangle = \alpha|0\rangle - \beta|1\rangle$. Then we have

$$\begin{aligned}|\Psi\rangle\langle\Psi| \otimes \mathbf{Tr}\left(|E\rangle\langle E|\right) &= |\alpha|^2|0\rangle\langle 0| + (1-2p)(\alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0|) + |\beta|^2|1\rangle\langle 1| \\ &= (1-p)\left(|\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\right) \\ &\quad + p\left(|\alpha|^2|0\rangle\langle 0| - \alpha\beta^*|0\rangle\langle 1| - \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|\right) \\ &= (1-p)|\Psi\rangle\langle\Psi| + pZ|\Psi\rangle\langle\Psi|Z\end{aligned}$$

So $|\Psi\rangle\langle\Psi| \to (1-p)|\Psi\rangle\langle\Psi| + pZ|\Psi\rangle\langle\Psi|Z$.
Note that $|E_i\rangle\langle E_i| \geq 0$ since $\langle u|E_i\rangle\langle E_i|u\rangle = |\langle u|E_i\rangle|^2 \geq 0$ for any $|u\rangle$ and $\lambda_{\max}(|E_i\rangle\langle E_i|) \leq 1$ since $\sum_i \lambda_i(|E_i\rangle\langle E_i|) = \mathbf{Tr}\left(|E_i\rangle\langle E_i|\right) = 1$ and $\lambda_j(|E_i\rangle\langle E_i|) \geq 0$. Then by problem 2(b) we have

$$|\langle E_0|E_1\rangle|^2 = \mathbf{Tr}\left(|E_0\rangle\langle E_0|E_1\rangle\langle E_1|\right) \leq \lambda_{\max}(|E_1\rangle\langle E_1|)\mathbf{Tr}\left(|E_0\rangle\langle E_0|\right) \leq 1.$$

Then we have $|\langle E_0|E_1\rangle| \leq 1$ which implies $0 \leq p \leq 1$ so p is a valid probability.