CS/Ph120 Homework 3 Solutions

November 3, 2016

Problem 1: Superdense Coding

Solution: (Due to Bolton Bailey)

(a) The most general way in which Bob can try to ascertain Alice's classical bits is by creating a POVM with four operators, each corresponding to a single guess for Alice's pair of qubits. Thus, we want a POVM

$$\{M_0, M_1, M_+, M_-\}$$

Which maximizes the value

$$\begin{aligned} &\frac{P(0|0) + P(1|1) + P(+|+) + P(-|-)}{4} \\ = &\frac{tr(M_0|0\rangle\langle 0|) + tr(M_1|1\rangle\langle 1|) + tr(M_+|+\rangle\langle +|) + tr(M_-|-\rangle\langle -|)}{4} \\ = &\frac{\langle 0|M_0|0\rangle + \langle 1|M_1|1\rangle + \langle +|M_+|+\rangle + \langle -|M_-|-\rangle}{4} \end{aligned}$$

And we want to know this maximal value. Observe that

$$\langle 0|M_0|0\rangle + \langle 1|M_1|1\rangle \leq \langle 0|M_0|0\rangle + \langle 1|M_0|1\rangle + \langle 0|M_1|0 + \langle 1|M_1|1 = tr(M_0 + M_1)$$

From the positive definiteness of these matrices, and similarly

$$\langle +|M_+|+\rangle + \langle -|M_-|-\rangle \leq \langle +|M_+|+\rangle + \langle -|M_+|-\rangle + \langle +|M_-| + +\langle -|M_-|- = tr(M_+ + M_-)$$

And we therefore have

$$\begin{aligned} \langle 0|M_0|0\rangle + \langle 1|M_1|1\rangle + \langle +|M_+|+\rangle + \langle -|M_-|-\rangle &\leq tr(M_0 + M_1) + tr(M_+ + M_-) \\ &= tr(M_0 + M_1 + M_+ + M_-) \\ &= tr(\mathbb{I}) \\ &= 2 \end{aligned}$$

And so

$$\begin{aligned}
&\frac{P(0|0)+P(1|1)+P(+|+)+P(-|-)}{4}\\
&=\frac{tr(M_0|0\rangle\langle 0|)+tr(M_1|1\rangle\langle 1|)+tr(M_+|+\rangle\langle +|)+tr(M_-|-\rangle\langle -|)}{4}\\
&=\frac{\langle 0|M_0|0\rangle+\langle 1|M_1|1\rangle+\langle +|M_+|+\rangle+\langle -|M_-|-\rangle}{4}\\
&\leq\frac{2}{4}\\
&=\frac{1}{2}
\end{aligned}$$

And so $\frac{1}{2}$ is an upper bound on the probability of success. We can attain this upper bound with

$$M_0 = |0\rangle\langle 0|$$

$$M_1 = |1\rangle\langle 1|$$

$$M_+ = 0$$

$$M_- = 0$$

Which measures in the standard basis. Thus, $\frac{1}{2}$ is the maximum value with which Bob can correctly guess both of Alices two classical bits.

(b) Initially the Alice-Bob Qubit pair is maximally entangled

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)$$

Suppose Alice applies one of the four unitary transformations

$$\{\mathbb{I}, X, Z, ZX\}$$

To her bit and then sends it to Bob. Now, Bob has the qubit pair state

$$\frac{1}{\sqrt{2}}((Z^{k_1}X^{k_2}|0\rangle_A)\otimes|0\rangle_B+(Z^{k_1}X^{k_2}|1\rangle_A)\otimes|1\rangle_B)$$

$$\frac{1}{\sqrt{2}}((Z^{k_1}X^{k_2}|0\rangle_A)\otimes|0\rangle_B+(Z^{k_1}X^{k_2}|1\rangle_A)\otimes|1\rangle_B)$$

Now, consider the possible values for this pair

$$|\psi\rangle_{00}\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)$$

$$|\psi\rangle_{01}\frac{1}{\sqrt{2}}(|1\rangle_A|0\rangle_B+|0\rangle_A|1\rangle_B)$$

$$|\psi\rangle_{10}\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\psi\rangle_{11}\frac{1}{\sqrt{2}}(-|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B)$$

This quadruple constitutes a basis. We can see this since all the states are normalized, and the two pairs of states which share components in the standard basis, their inner products evaluate to 0. Thus, all Bob has to do is to measure his state in this basis, thereby ascertaining which of the four states

(c) No, Eve cannot recover any information about the classical bits Alice is sharing with Bob. To see this, we trace out Bob's bit from the two qubit state, leaving only the intercepted qubit. Letting U_A be the unitary applied by Alice, the density matrix for Alice and Bob's state is

$$\frac{1}{2}(U_A|0\rangle_A)(\langle 0|_A U^\dagger) \otimes |0\rangle_B\langle 0|_B +$$
$$\frac{1}{2}(U_A|0\rangle_A)(\langle 1|_A U^\dagger) \otimes |0\rangle_B\langle 1|_B +$$
$$\frac{1}{2}(U_A|1\rangle_A)(\langle 0|_A U^\dagger) \otimes |1\rangle_B\langle 0|_B +$$
$$\frac{1}{2}(U_A|1\rangle_A)(\langle 1|_A U^\dagger) \otimes |1\rangle_B\langle 1|_B$$

And so if we trace out the second bit, we get

$$\frac{1}{2}[(U_A|0\rangle_A)(\langle 0|_A U^\dagger) + (U_A|1\rangle_A)(\langle 1|_A U^\dagger)]$$

$$= U_A(\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|))U_A^\dagger$$

$$= U_A\frac{\mathbb{I}}{2}U_A^\dagger$$

Now, neither the application of X or Z change the value of the maximally mixed state $\frac{\mathbb{I}}{2}$, so whatever Alice's bits are, Eve's state is maximally mixed, and so she learns nothing.

Problem 2: Semidefinite Programming

Solution: (Due to De Huang)

(a) We first prove a Lemma: If $X, Y \in M_d(\mathbb{C})$, $X \geq 0, Y \geq 0$, then $tr(XY) \geq 0$.

Proof: Consider the eigenvalue decomposition of X,

$$X = Q\Lambda Q^\dagger,$$

where Q is unitary, and Λ is a diagonal matrix with diagonal elements $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_d \geq 0$. Then

$$tr(XY) = tr(Q\Lambda Q^\dagger Y) = tr(\Lambda Q^\dagger Y Q).$$

Let $s_1, s_2, \ldots, s_d$ be the diagonal elements of $Q^\dagger Y Q$. Since $Y \geq 0$, we have $Q^\dagger Y Q \geq 0$, and thus $s_i \geq 0,\ i = 1, 2, \ldots, d$. Therefore

$$tr(XY) = tr(\Lambda Q^\dagger Y Q) = \sum_{i=1}^{d} \lambda_i s_i \geq 0.$$

Let $\Omega_1 = \{X \in M_d(\mathbb{C}) : X \geq 0, \Phi(X) = B\}$, $\Omega_2 = \{Y \in M_{d'}(\mathbb{C}) : \Phi^*(Y) \geq A, Y = Y^\dagger)$. Now given any $X \in \Omega_1, Y \in \Omega_2$, we have

$$\begin{aligned} tr(BY) &= tr(\Phi(X)Y) \\ &= tr(\sum_{i=1}^{k} K_i X K_i^\dagger Y) \\ &= tr(\sum_{i=1}^{k} X K_i^\dagger Y K_i) \\ &= tr(X\Phi^*(Y)). \end{aligned}$$

Since $\Phi^*(Y) \geq A$, i.e. $\Phi^*(Y) - A \geq 0$, using the Lemma we have

$$tr(X(\Phi^*(Y) - A)) \geq 0,$$

$$\Rightarrow \quad tr(BY) = tr(X\Phi^*(Y)) \geq tr(XA) = tr(AX).$$

Since X, Y are arbitrary in Ω_1, Ω_2, we immediately have

$$\beta = \min_{Y \in \Omega_2} tr(BY) \geq \max_{X \in \Omega_1} tr(AX) = \alpha.$$

(b) Consider the eigenvalue decomposition of M,

$$M = U \Lambda U^\dagger,$$

where U is unitary, and and Λ is a diagonal matrix with diagonal elements $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_d$. We have

$$\lambda \mathbb{I} \geq M \quad \Rightarrow \quad \lambda \mathbb{I} - M \geq 0 \quad \Rightarrow \quad U^\dagger(\lambda \mathbb{I} - M)U \geq 0 \quad \Rightarrow \quad \lambda \mathbb{I} - \Lambda \geq 0.$$

Notice that $\lambda \mathbb{I} - \Lambda$ is a diagonal matrix. Thus we have $\lambda - \lambda_i \geq 0,\ i = 1, 2, \ldots, d$, which means all eigenvalues of M are less than or equal to λ.

(c) We can choose that $A = M \in M_d(\mathbb{C}), B = 1 \in \mathbb{C}$, and each $K_i, i = 1, 2, \ldots, d$ is a $1 \times d$ vector such that the i_{th} element is 1 and the other elements are 0. Then for any $X \in M_d(\mathbb{C})$ and any $y \in \mathbb{C}$, we have

$$\Phi(X) = \sum_{i=1}^{d} K_i X K_i^\dagger = \sum_{i=1}^{d} X_{ii} = tr(X),$$

$$\Phi^*(y) = \sum_{i=1}^{d} K_i^\dagger y K_i = y\mathbb{I}.$$

Now we have $tr(By) = y$, and $y = y^\dagger \Rightarrow y \in \mathbb{R}$. Then the dual problem is just

$$\beta = \min_{y \in \mathbb{R}} y$$

$$s.t. \quad y\mathbb{I} \geq M.$$

Using the result of (b), it's easy to see that $\beta = \lambda_1(M)$. The primal problem is

$$\alpha = \max_{X} tr(MX)$$

$$s.t. \quad tr(X) = 1,$$

$$X \geq 0.$$

Given $X \geq 0$, we can always find the root decomposition of X,

$$X = PP^\dagger.$$

Let p_i denote the i_{th} column of P, then we have

$$tr(MX) = tr(MPP^\dagger) = tr(P^\dagger MP) = \sum_{i=1}^{d} p_i^\dagger M p_i,$$

and

$$1 = tr(X) = tr(PP^\dagger) = tr(P^\dagger P) \quad \Rightarrow \quad \sum_{i=1}^{d} \|p_i\|_2 = 1.$$

Thus the primal problem is equivalent to

$$\alpha = \max_{p_i, i=1,2,\ldots,d} \sum_{i=1}^{d} p_i^\dagger M p_i$$

$$s.t. \quad \sum_{i=1}^{d} \|p_i\|_2 = 1.$$

Since given that M is Hermitian, for any feasible $p_i, i = 1, 2, \ldots, d$, we have

$$\sum_{i=1}^{d} p_i^\dagger M p_i \leq \sum_{i=1}^{d} \lambda_1(M) p_i^\dagger p_i = \lambda_1(M) \sum_{i=1}^{d} \|p_i\|_2 = \lambda_1(M).$$

Thus $\alpha \leq \lambda_1(M)$. In particular, if we choose p_1 to be the normalized eigenvector of M associated with $\lambda_1(M)$, and $p_i = 0, i = 2, 3, \ldots, d$, then

$$\sum_{i=1}^{d} \|p_i\|_2 = 1, \quad \sum_{i=1}^{d} p_i^\dagger M p_i = p_1^\dagger M p_1 = \lambda_1(M).$$

Therefore we have $\alpha = \lambda_1(M) = \beta$.

(d) Recall that in class we have shown that

$$\|\rho-\sigma\|_{tr} = \max_{E_1,E_2}\ tr(\rho E_1)+tr(\sigma E_2)-1$$

$$s.t.\quad E_1\geq 0,\ E_2\geq 0,$$

$$E_1+E_2=\mathbb{I},$$

given that ρ,σ are density matrices. Let

$$A=\begin{pmatrix}\rho & \\ & \sigma\end{pmatrix}\in M_{2d}(\mathbb{C}),\quad B=\mathbb{I}\in M_d(\mathbb{C}),$$

$$K_1=\begin{pmatrix}\mathbb{I} & 0\end{pmatrix}\in M_{d\times 2d}(\mathbb{C}),\quad K_2=\begin{pmatrix}0 & \mathbb{I}\end{pmatrix}\in M_{d\times 2d}(\mathbb{C}).$$

Consider the two sets $\Omega_1=\{(E_1,E_2)\in(M_d(\mathbb{C}),M_d(\mathbb{C})):E_1\geq 0,E_2\geq 0,E_1+E_2=\mathbb{I}\}$, $\Omega_2=\{X\in M_{2d}(\mathbb{C}):X\geq 0,\Phi(X)=\mathbb{I}\}$. For any matrix

$$X=\begin{pmatrix}X_1 & X_3\\ X_3^\dagger & X_2\end{pmatrix}\in\Omega_2,$$

let $E_1=X_1,E_2=X_2$, then we have

$$tr(AX)=tr(\rho E_1)+tr(\sigma E_2),$$

and $(E_1,E_2)\in\Omega_1$, because

$$X\geq 0\quad\Rightarrow\quad E_1\geq 0,\ E_2\geq 0,$$

$$\Phi(X)=B=\mathbb{I}\quad\Rightarrow\quad K_1XK_1^\dagger+K_2XK_2^\dagger=E_1+E_2=\mathbb{I}.$$

Conversely, for any $(E_1,E_2)\in\Omega_1$, let

$$X=\begin{pmatrix}E_1 & 0\\ 0 & E_2\end{pmatrix},$$

then we have

$$tr(AX)=tr(\rho E_1)+tr(\sigma E_2),$$

and $X\in\Omega_2$, because

$$E_1\geq 0,\ E_2\geq 0\quad\Rightarrow\quad X\geq 0,$$

$$E_1+E_2=\mathbb{I}\quad\Rightarrow\quad\Phi(X)=K_1XK_1^\dagger+K_2XK_2^\dagger=\mathbb{I}=B.$$

Therefore if we consider the primal problem

$$\alpha=\max_X\ tr(AX)-1$$

$$s.t.\quad\Phi(X)=B,$$

$$X\geq 0,$$

it's easy to see that $\alpha=\|\rho-\sigma\|_{tr}=\|M\|_{tr}$. Notice that this primal problem with a '-1' in the objective function is a little different from the original form above, but we can fix this by simply adding one more dimension to the problem, which would have more complicated expressions for A, B, K_1, K_2. For convenience, we just stick to this modified primal problem.

Now the modified dual problem

$$\begin{aligned} \beta = \min_{Y} \ & tr(BY) - 1 \\ s.t. \quad & \Phi^*(Y) \geq A, \\ & Y = Y^\dagger, \end{aligned}$$

is equivalent to

$$\begin{aligned} \beta = \min_{Y} \ & tr(Y) - 1 \\ s.t. \quad & Y \geq \rho, \ Y \geq \sigma, \\ & Y = Y^\dagger. \end{aligned}$$

which can be easily verified by substuting the explict expressions of A, B, K_1, K_2 into the modified dual problem.

Next we need to prove in this case $\beta = \alpha = \|\rho - \sigma\|_{tr}$. Since in (a) we already showed that $\alpha \leq \beta$, we only need to show that there exists a feasible Y such that $tr(Y) - 1 = \alpha = \|\rho - \sigma\|_{tr}$. Consider the eigenvalue decomposition of $\rho - \sigma$,

$$\rho - \sigma = Q \Lambda Q^\dagger,$$

where Q is unitary, and and Λ is a diagonal matrix with diagonal elements

$$\lambda_1 \geq \lambda_2 \ldots \geq \lambda_r \geq 0 > \lambda_{r+1} \geq \ldots \geq \lambda_d.$$

Since ρ, σ are density matrices, we have

$$\|\rho - \sigma\|_{tr} = \sum_{i=1}^{r} \lambda_i = \frac{1}{2} \sum_{i=1}^{d} |\lambda_i| = \frac{1}{2} \sum_{i=1}^{r} \lambda_i - \frac{1}{2} \sum_{i=r+1}^{d} \lambda_i.$$

Let q_i denote the i_{th} column of Q. Now define

$$s_i = q_i^\dagger \rho q_i, \quad i = 1, 2, \ldots, d,$$

$$t_i = q_i^\dagger \sigma q_i, \quad i = 1, 2, \ldots, d.$$

We have

$$s_i - t_i = q_i^\dagger (\rho - \sigma) q_i = \lambda_i \geq 0, \quad i = 1, 2, \ldots, r,$$
$$t_i - s_i = -q_i^\dagger (\rho - \sigma) q_i = -\lambda_i > 0, \quad i = r+1, r+2, \ldots, d.$$

Let S, T, Σ be three diagonal matrices such that their diagonal vectors are $(s_1, s_2, \ldots, s_d)$, $(t_1, t_2, \ldots, t_d)$ and $(s_1, s_2, \ldots, s_r, t_{r+1}, t_{r+2}, \ldots, t_d)$ respectively. Then

$$\Sigma - S = \text{diag}(0, 0, \ldots, 0, t_{r+1} - s_{r+1}, \ldots, t_d - s_d) \geq 0,$$

$$\Sigma - T = \text{diag}(s_1 - t_1, s_2 - t_2, \ldots, s_r - t_r, 0, \ldots, 0) \geq 0,$$

where $\text{diag}(v)$ denotes the diagonal matrix with diagonal vactor v. Notice that S and T are the diagonal parts of $Q^\dagger \rho Q$ and $Q^\dagger \sigma Q$ respectively. We should also notice that

$$q_i^\dagger (\rho - \sigma) q_j = 0, \quad i \neq j,$$

which means the non-diagonal part of $Q^\dagger \rho Q$ and $Q^\dagger \sigma Q$ are the same, i.e.

$$Q^\dagger \rho Q - S = Q^\dagger \sigma Q - T \triangleq L.$$

Now we have

$$Q^\dagger \rho Q = S + L, \quad Q^\dagger \sigma Q = T + L.$$

Let

$$Y = Q(\Sigma + L)Q^\dagger.$$

Obviously $Y = Y^\dagger$, and we have

$$Q^\dagger (Y - \rho) Q = \Sigma + L - S - L = \Sigma - S \geq 0 \quad \Rightarrow \quad Y \geq \rho,$$

$$Q^\dagger (Y - \sigma) Q = \Sigma + L - T - L = \Sigma - T \geq 0 \quad \Rightarrow \quad Y \geq \sigma,$$

thus Y is a feasible solution to the dual problem. Moreover, notice that we have

$$\sum_{i=1}^{d} s_i = tr(Q^\dagger \rho Q) = tr(\rho) = 1, \quad \sum_{i=1}^{d} t_i = tr(Q^\dagger \sigma Q) = tr(\sigma) = 1,$$

therefore

$$tr(Y) = tr(\Sigma) = \sum_{i=1}^{r} s_i + \sum_{i=r+1}^{d} t_i = \sum_{i=1}^{r} (s_i - t_i) + \sum_{i=1}^{d} t_i = \sum_{i=1}^{r} \lambda_i + 1 = \|\rho - \sigma\|_{tr} + 1,$$

that is $\beta \leq tr(Y) - 1 = \|\rho - \sigma\|_{tr} = \alpha$. In all we have $\beta = \alpha = \|\rho - \sigma\|_{tr}$.

(e) The success probability of distinguishing with a POVM $\{M_x\}$ is

$$\sum_{i=1}^{k} p_i \mathbf{Pr}(M_i | \rho_i) = \sum_{i=1}^{k} p_i tr(M_i \rho_i).$$

Define

$$A = \begin{pmatrix} p_1 \rho_1 & & & \\ & p_2 \rho_2 & & \\ & & \ddots & \\ & & & p_k \rho_k \end{pmatrix} \in M_{kd}(\mathbb{C}), \quad B = \mathbb{I} \in M_d(\mathbb{C}),$$

$$K_i = (0, \ldots, 0, \underset{i_{\text{th}} \text{ block}}{\mathbb{I}}, 0, \ldots, 0) \in M_{d \times kd}(\mathbb{C}), \quad i = 1, 2, \ldots, k.$$

then using the similar argument in (d), we can see that solving the optimization problem

$$\alpha = \max_{M_x} \sum_{i=1}^{k} p_i tr(M_i \rho_i)$$

$$
\begin{aligned}
s.t.\quad & M_i \geq 0,\ i = 1, 2, \ldots, k,\\
& \sum_{i=1}^{k} M_i = \mathbb{I},
\end{aligned}
$$

is equivalent to solving the primal problem

$$
\alpha = \max_{X}\ tr(AX)
$$

$$
\begin{aligned}
s.t.\quad & \Phi(X) = B,\\
& X \geq 0,
\end{aligned}
$$

and given an optimal solution X^* for the primal problem, we can recover a optimal solution $\{M_i^*\}_{1\geq i\geq k}$ for the first problem by taking $\{M_i^*\}_{1\geq i\geq k}$ to be the diagonal blocks of X^*. Indeed, let Ω_1 and Ω_2 be the feasible sets of the two problems above respectively. For any $\{M_i\}_{1\geq i\geq k} \in \Omega_1$, let

$$
X = \begin{pmatrix} M_1 & & & \\ & M_2 & & \\ & & \ddots & \\ & & & M_k \end{pmatrix},
$$

then we have

$$
tr(AX) = \sum_{i=1}^{k} p_i tr(M_i \rho_i), \quad K_i X K_i^\dagger = M_i, \quad i = 1, 2, \ldots, k,
$$

and $X \in \Omega_2$ because

$$
\begin{aligned}
\sum_{i=1}^{k} M_i = \mathbb{I} \quad &\Rightarrow \quad \Phi(X) = B = \mathbb{I},\\
M_i \geq 0,\ i = 1, 2, \ldots, k \quad &\Rightarrow \quad X \geq 0.
\end{aligned}
$$

Conversely, for any $X \in \Omega_2$, let $M_1, M_2, \ldots, M_k$ be the diagonal blocks of X, then we have

$$
\sum_{i=1}^{k} p_i tr(M_i \rho_i) = tr(AX), \quad K_i X K_i^\dagger = M_i, \quad i = 1, 2, \ldots, k,
$$

and $\{M_i\}_{1\geq i\geq k} \in \Omega_1$ because

$$
\Phi(X) = B = \mathbb{I} \quad \Rightarrow \quad \sum_{i=1}^{k} M_i = \mathbb{I},
$$

$$
X \geq 0 \quad \Rightarrow \quad M_i \geq 0,\ i = 1, 2, \ldots, k.
$$

Problem 3: Maximally entangled properties

Solution: (Due to Bolton Bailey)

(i) We have a maximally entangled pair of qubits

$$|\Phi^+\rangle = \sum_{0\leq i\leq d-1} \frac{1}{\sqrt{d}} |i\rangle_A \otimes |i\rangle_B$$

To find the reduced state on A we trace out the B system

$$\begin{aligned}
Tr_B(|\Phi^+\rangle\langle\Phi^+|) &= Tr_B\left(\sum_{0\leq i,j\leq d-1} \frac{1}{d}(|i\rangle_A \otimes |i\rangle_B)(\langle j|_A \otimes \langle j|_B)\right) \\
&= \sum_{0\leq i,j\leq d-1} \frac{1}{d} Tr_B\left((|i\rangle_A \otimes |i\rangle_B)(\langle j|_A \otimes \langle j|_B)\right) \\
&= \sum_{0\leq i,j\leq d-1} \frac{1}{d} Tr_B\left((|i\rangle_A\langle j|_A \otimes |i\rangle_B\langle j|_B)\right) \\
&= \sum_{0\leq i\leq d-1} \frac{1}{d} |i\rangle_A\langle i|_A
\end{aligned}$$

So we get the maximally mixed state on the A system.
(ii) $M \otimes \mathbb{I}$ and $\mathbb{I} \otimes M^T$ are both $d^2 \times d^2$ matrices, and $|\Phi^+\rangle$ is a vector of length d^2, so $M \otimes \mathbb{I}|\Phi^+\rangle$ and $\mathbb{I} \otimes M^T|\Phi^+\rangle$ are vectors of length d^2. To see these are equal, we must show their components are equal. That is, for each $0 \leq k, l \leq d-1$, we must show

$$(\langle k| \otimes \langle l|)M \otimes \mathbb{I}|\Phi^+\rangle = (\langle k| \otimes \langle l|)\mathbb{I} \otimes M^T|\Phi^+\rangle$$

Now see

$$\begin{aligned}
(\langle k| \otimes \langle l|)M \otimes \mathbb{I}|\Phi^+\rangle &= (\langle k| \otimes \langle l|)M \otimes \mathbb{I}\left(\sum_{0\leq i\leq d-1} \frac{1}{\sqrt{d}} |i\rangle_A \otimes |i\rangle_B\right) \\
&= \sum_{0\leq i\leq d-1} \frac{1}{\sqrt{d}} ((\langle k| \otimes \langle l|)M \otimes \mathbb{I}\,(|i\rangle_A \otimes |i\rangle_B) \\
&= \sum_{0\leq i\leq d-1} \frac{1}{\sqrt{d}} \langle k|M|i\rangle \otimes \langle l|\mathbb{I}|i\rangle \\
&= \sum_{0\leq i\leq d-1} \frac{1}{\sqrt{d}} \langle k|M|i\rangle \otimes \langle l|i\rangle \\
&= \frac{1}{\sqrt{d}} \langle k|M|l\rangle \\
&= \frac{1}{\sqrt{d}} M_{kl}
\end{aligned}$$

And

$$\begin{aligned}
(\langle k| \otimes \langle l|)\mathbb{I} \otimes M^T|\Phi^+\rangle &= (\langle k| \otimes \langle l|)\mathbb{I} \otimes M^T \left(\sum_{0\le i\le d-1} \frac{1}{\sqrt{d}}|i\rangle_A \otimes |i\rangle_B\right) \\
&= \sum_{0\le i\le d-1} \frac{1}{\sqrt{d}}(\langle k| \otimes \langle l|)\mathbb{I} \otimes M^T \left(|i\rangle_A \otimes |i\rangle_B\right) \\
&= \sum_{0\le i\le d-1} \frac{1}{\sqrt{d}}\langle k|\mathbb{I}|i\rangle \otimes \langle l|M^T|i\rangle \\
&= \sum_{0\le i\le d-1} \frac{1}{\sqrt{d}}\langle k|i\rangle \otimes \langle l|M^T|i\rangle \\
&= \frac{1}{\sqrt{d}}M^T_{lk} \\
&= \frac{1}{\sqrt{d}}M_{kl}
\end{aligned}$$

So these two are indeed equal.

Problem 4: Choi's Theorem

Solution: (Due to De Huang)

(a) Assume that (2) is true, i.e.

$$\boldsymbol{T}(X) = \sum_s K_s X K_s^\dagger, \quad \forall X \in M_d(\mathbb{C}).$$

For any $d'' \ge 0$ and any $X \otimes Y \in M_d(\mathbb{C}) \otimes M_{d''}(\mathbb{C})$ such that $X \otimes Y \ge 0$, we have

$$\boldsymbol{T} \otimes \boldsymbol{id_{d''}}(X \otimes Y) = T(X) \otimes Y = \sum_s K_s X K_s^\dagger \otimes Y.$$

Then for any joint state

$$|\Phi\rangle = \sum_{0\le i\le d-1}\sum_{0\le j\le d''-1} a_{ij}|i\rangle \otimes |j\rangle \in \operatorname{span}\{\mathbb{C}^d \otimes \mathbb{C}^{d''}\},$$

we have

$$
\begin{aligned}
\langle\Phi|\boldsymbol{T}\otimes\boldsymbol{id_{d''}}(X\otimes Y)|\Phi\rangle &= \sum_s\langle\Phi|(K_sXK_s^\dagger\otimes Y)|\Phi\rangle \\
&= \sum_s\sum_{i,j}\sum_{k,l}\overline{a_{ij}}a_{kl}\langle i|K_sXK_s^\dagger|k\rangle\langle j|Y|l\rangle \\
&= \sum_s\Big(\sum_{i,j}\overline{a_{ij}}(\langle i|K_s)\otimes\langle j|\Big)(X\otimes Y)\Big(\sum_{i,j}a_{ij}(K_s^\dagger|i\rangle)\otimes|j\rangle\Big) \\
&= \sum_s\big(\langle\Phi|K_s\otimes\mathbb{I}\big)(X\otimes Y)\big(K_s^\dagger\otimes\mathbb{I}|\Phi\rangle\big) \\
&\geq 0.
\end{aligned}
$$

Since $|\Phi\rangle$ is arbitrary, we have $\boldsymbol{T}\otimes\boldsymbol{id_{d''}}(X\otimes Y)\geq 0$. And since d'' and $X\otimes Y$ are arbitrary, we can conclude that $\boldsymbol{T}$ is completely positive.

(b) (3)⇒(1) is trival. If $\boldsymbol{T}$ is completely positive, then by definition, in the case $d''=d$, $\boldsymbol{T}\otimes\boldsymbol{id_d}$ is positive. Since $\Phi^+=|\Phi^+\rangle\langle\Phi^+|$ is positive semidefinite, we immediately have that

$$J(\boldsymbol{T})=\boldsymbol{T}\otimes\boldsymbol{id_d}(\Phi^+)$$

is positive semidefinite.

(c) We may always assume that

$$X|j\rangle=\sum_{0\leq j\leq d-1}x_{ij}|i\rangle,$$

then we can write X as

$$X=\sum_{0\leq i,j\leq d-1}x_{ij}|i\rangle\langle j|,$$

and we have

$$T(X)=\sum_{0\leq i,j\leq d-1}x_{ij}T(|i\rangle\langle j|).$$

On the other hand, we have

$$
\begin{aligned}
\big(\boldsymbol{id_{d'}}\otimes\boldsymbol{t_d}(J(\boldsymbol{T}))\big)(\mathbb{I}\otimes X) &= \big(\sum_{0\leq i,j\leq d-1}\boldsymbol{T}(|i\rangle\langle j|)\otimes\boldsymbol{t_d}(|i\rangle\langle j|)\big)(\mathbb{I}\otimes X) \\
&= \sum_{0\leq i,j\leq d-1}\big(\boldsymbol{T}(|i\rangle\langle j|)\otimes|j\rangle\langle i|\big)(\mathbb{I}\otimes X) \\
&= \sum_{0\leq i,j\leq d-1}\boldsymbol{T}(|i\rangle\langle j|)\otimes(|j\rangle\langle i|X) \\
&= \sum_{0\leq i,j\leq d-1}\boldsymbol{T}(|i\rangle\langle j|)\otimes\big(|j\rangle\langle i|(\sum_{0\leq k,l\leq d-1}x_{kl}|k\rangle\langle l|)\big) \\
&= \sum_{0\leq i,j\leq d-1}\boldsymbol{T}(|i\rangle\langle j|)\otimes\big(\sum_{0\leq l\leq d-1}x_{il}|j\rangle\langle l|\big) \\
&= \sum_{0\leq i,j,l\leq d-1}x_{il}\boldsymbol{T}(|i\rangle\langle j|)\otimes|j\rangle\langle l|,
\end{aligned}
$$

and thus

$$\begin{aligned} tr_A\Big(\big(\boldsymbol{id_{d'}}\otimes\boldsymbol{t_d}(J(\boldsymbol{T}))\big)(\mathbb{I}_B\otimes X_A)\Big) &= tr_A\Big(\sum_{0\le i,j,l\le d-1} x_{il}\boldsymbol{T}(|i\rangle\langle j|)_B\otimes|j\rangle\langle l|_A\Big)\\ &= \sum_{0\le i,j\le d-1} x_{ij}\boldsymbol{T}(|i\rangle\langle j|)\\ &= T(X). \end{aligned}$$

Now we can define a bidirectional map between linear map $\boldsymbol{T}$ from $M_d(\mathbb{C})$ to $M_{d'}(\mathbb{C})$ and their operator representation $J(\boldsymbol{T})$ in $M_{d'}(\mathbb{C})\otimes M_d(\mathbb{C})$. One direction is

$$\boldsymbol{T}\ \rightarrow\ J(\boldsymbol{T}),$$

and the other direction is

$$J(\boldsymbol{T})\ \rightarrow\ tr_A\Big(\big(\boldsymbol{id_{d'}}\otimes\boldsymbol{t_d}(J(\boldsymbol{T}))\big)(\mathbb{I}_B\otimes(\ \cdot\ )_A)\Big)=\boldsymbol{T}(\ \cdot\ ).$$

These two directions are inverse to each other, so this is a one-to-one map. Let's define $J^{-1}(J(\boldsymbol{T}))=\boldsymbol{T}$ for future use. Also we can see that both J and J^{-1} are linear.

(d) For an arbitrary $Z\in M_{d'\times d}$,

$$Z=\sum_{0\le i\le d'-1}\sum_{0\le j\le d-1} a_{ij}|i\rangle\langle j|,$$

we have

$$\begin{aligned} \boldsymbol{vec}(Z) &= \sum_{0\le i\le d'-1}\sum_{0\le j\le d-1} a_{ij}\boldsymbol{vec}(|i\rangle\langle j|)\\ &= \sum_{0\le i\le d'-1}\sum_{0\le j\le d-1} a_{ij}|i\rangle\otimes|j\rangle\\ &= \sum_{0\le j\le d-1}\big(\sum_{0\le i\le d'-1} a_{ij}|i\rangle\big)\otimes|j\rangle\\ &= \sum_{0\le j\le d-1} Z|j\rangle\otimes|j\rangle, \end{aligned}$$

where we have used the fact that

$$Z|j\rangle=\sum_{0\le i\le d'-1} a_{ij}|i\rangle,\quad 0\le j\le d-1.$$

Therefore we have

$$\begin{aligned} J(\boldsymbol{T}) &= \boldsymbol{T} \otimes \boldsymbol{id_d}(\Phi^+) \\ &= \sum_{0 \le i,j \le d-1} \boldsymbol{T}(|i\rangle\langle j|) \otimes |i\rangle\langle j| \\ &= \sum_{0 \le i,j \le d-1} (Z|i\rangle\langle j|Z^\dagger) \otimes |i\rangle\langle j| \\ &= \sum_{0 \le i,j \le d-1} \big((Z|i\rangle) \otimes |i\rangle\big)\big((\langle j|Z^\dagger) \otimes \langle j|\big) \\ &= \Big(\sum_{0 \le i \le d-1} (Z|i\rangle) \otimes |i\rangle\Big)\Big(\sum_{0 \le i \le d-1} (\langle j|Z^\dagger) \otimes \langle j|\Big) \\ &= |\zeta\rangle\langle\zeta|, \end{aligned}$$

with $|\zeta\rangle = \boldsymbol{vec}(Z)$.

(e) If (1) is true, $J(\boldsymbol{T})$ is positive semidefinite, we should be able to write $J(\boldsymbol{T})$ in form of its eigenvalue decomposition

$$J(\boldsymbol{T}) = \sum_s \lambda_s |\zeta_s\rangle\langle\zeta_s|,$$

where $\lambda_s > 0$ for each s, and each

$$|\zeta_s\rangle = \sum_{0 \le i \le d'-1} \sum_{0 \le j \le d-1} c_{ij}^s |i\rangle \otimes |j\rangle \in \mathrm{span}\{\mathbb{C}^{d'} \otimes \mathbb{C}^d\}$$

is an normalized eigenstate of $J(\boldsymbol{T})$. Let's define

$$Z_s = \sum_{0 \le i \le d'-1} \sum_{0 \le j \le d-1} c_{ij}^s |i\rangle\langle j|, \qquad \boldsymbol{T}_s = J^{-1}(|\zeta_s\rangle\langle\zeta_s|),$$

where the notation J^{-1} has been defined in (c). Then it's easy to check that

$$\boldsymbol{vec}(Z_s) = |\zeta_s\rangle, \quad J(\boldsymbol{T}_s) = |\zeta_s\rangle\langle\zeta_s|,$$

and using the result of (c) and (d) we have

$$\boldsymbol{T}_s(X) = Z_s X Z_s^\dagger, \quad \forall X \in M_d(\mathbb{C}).$$

Now we have

$$J(\boldsymbol{T}) = \sum_s \lambda_s |\zeta_s\rangle\langle\zeta_s| = \sum_s \lambda_s J(\boldsymbol{T}_s),$$

then by linearity we have

$$\boldsymbol{T} = J^{-1}(J(\boldsymbol{T})) = \sum_s \lambda_s J^{-1}(J(\boldsymbol{T}_s)) = \sum_s \lambda_s \boldsymbol{T}_s.$$

Further, since $\lambda_s > 0$ for each s, we can define

$$K_s = \sqrt{\lambda_s} Z_s,$$

then we have

$$\boldsymbol{T}(X) = \sum_s \lambda_s \boldsymbol{T}_s(X) = \sum_s \lambda_s Z_s X Z_s^\dagger = \sum_s K_s X K_s^\dagger, \quad \forall X \in M_d(\mathbb{C}),$$

which means (2) is true.

Problem 5: A limit on quantum attacks on Wiesner's scheme

Solution: (Due to De Huang)

(a) The success probability is

$$\mathbf{Pr}(success) = \frac{1}{4} \sum_{x,\theta\in\{0,1\}} tr\big(\boldsymbol{T}(|x\rangle\langle x|_\theta)(|x\rangle\langle x|_\theta \otimes |x\rangle\langle x|_\theta)\big).$$

(b) Notice that for any matrices $N \in M_4(\mathbb{C})$ and $M \in M_2(\mathbb{C})$, we have

$$\begin{aligned} tr\big(J(\boldsymbol{T})(N\otimes M)\big) &= \sum_{i,j\in\{0,1\}} tr\big((\boldsymbol{T}(|i\rangle\langle j|)\otimes|i\rangle\langle j|)(N\otimes M)\big) \\ &= \sum_{i,j\in\{0,1\}} tr\big(\boldsymbol{T}(|i\rangle\langle j|)N\otimes|i\rangle\langle j|M\big) \\ &= \sum_{i,j\in\{0,1\}} tr\big(\boldsymbol{T}(|i\rangle\langle j|)N\big)tr\big(|i\rangle\langle j|M\big) \\ &= \sum_{i,j\in\{0,1\}} tr\big(\boldsymbol{T}(|i\rangle\langle j|)N\big)m_{ij} \\ &= tr\big(\boldsymbol{T}(\sum_{i,j\in\{0,1\}} m_{ij}|i\rangle\langle j|)N\big) \\ &= tr\big(\boldsymbol{T}(M)N\big), \end{aligned}$$

where we have use that

$$M = \sum_{i,j\in\{0,1\}} m_{ij}|i\rangle\langle j|,$$

$$m_{ij} = \langle i|M|j\rangle = tr(|i\rangle\langle j|M), \quad i,j\in\{0,1\}.$$

Then using this result by taking $N = |x\rangle\langle x|_\theta \otimes |x\rangle\langle x|_\theta, M = |x\rangle\langle x|_\theta$ for each pair of (x,θ), we have

$$\begin{aligned} tr(J(\boldsymbol{T})Q) &= \sum_{x,\theta\in\{0,1\}} tr\big(J(\boldsymbol{T})(|x\rangle\langle x|_\theta\otimes|x\rangle\langle x|_\theta\otimes|x\rangle\langle x|_\theta)\big) \\ &= \sum_{x,\theta\in\{0,1\}} tr\big(\boldsymbol{T}(|x\rangle\langle x|_\theta)(|x\rangle\langle x|_\theta\otimes|x\rangle\langle x|_\theta)\big) \\ &= 4\mathbf{Pr}(success), \end{aligned}$$

that is

$$\mathbf{Pr}(success) = \frac{1}{4}tr(J(\boldsymbol{T})Q).$$

(c) If $\boldsymbol{T}$ is trace-preserving, then we have

$$\begin{aligned} tr_1\big(J(\boldsymbol{T})\big) &= \sum_{0\le i,j\le d-1} tr\big(\boldsymbol{T}(|i\rangle\langle j|)\big)|i\rangle\langle j| \\ &= \sum_{0\le i,j\le d-1} \delta_{ij}|i\rangle\langle j| \\ &= \sum_{0\le i\le d-1} |i\rangle\langle i| \\ &= \mathbb{I}_d. \end{aligned}$$

Conversely, if we have

$$\sum_{0\le i,j\le d-1} tr\big(\boldsymbol{T}(|i\rangle\langle j|)\big)|i\rangle\langle j| = \mathbb{I}_d,$$

then

$$\delta_{ij} = \langle i|\mathbb{I}_d|j\rangle = \langle i|\Big(\sum_{0\le k,l\le d-1} tr\big(\boldsymbol{T}(|k\rangle\langle l|)\big)|k\rangle\langle l|\Big)|j\rangle = tr\big(\boldsymbol{T}(|i\rangle\langle j|)\big), \quad \forall 0\le i,j\le d-1.$$

Therefore for any

$$X = \sum_{0\le i,j\le d-1} x_{ij}|i\rangle\langle j| \in M_d(\mathbb{C}),$$

we have

$$\begin{aligned} tr\big(\boldsymbol{T}(X)\big) &= tr\big(\sum_{0\le i,j\le d-1} x_{ij}T(|i\rangle\langle j|)\big) \\ &= \sum_{0\le i,j\le d-1} x_{ij}tr\big(T(|i\rangle\langle j|)\big) \\ &= \sum_{0\le i\le d-1} x_{ii} \\ &= tr(X). \end{aligned}$$

Since X is arbitrary, we may conclude that $\boldsymbol{T}$ is trace-preserving.

(d) Recall in (b) we have shown that

$$\mathbf{Pr}(success(\boldsymbol{T})) = \frac{1}{4}tr\big(QJ(\boldsymbol{T})\big),$$

so we may take $A = \frac{1}{4}Q$, and the variable $X = J(\boldsymbol{T})$. After obtaining the optimal X^*, we may recover the optimal $\boldsymbol{T}^*$ as $\boldsymbol{T}^* = J^{-1}(X^*)$, where J^{-1} is defined in problem 4 (c) as

$$J^{-1}(X)(\,\cdot\,) = tr_A\Big(\big(\boldsymbol{id_4}\otimes \boldsymbol{t_2}(X)\big)(\mathbb{I}_B\otimes(\,\cdot\,)_A\Big).$$

Define

$$K_{ij} = \langle i|\langle j|\otimes \mathbb{I}_2, \quad i,j\in\{0,1\},$$

$$\Phi(X) = \sum_{i,j\in\{0,1\}} K_{ij} X K_{ij}^{\dagger},$$

then for any matrices $N \in M_4(\mathbb{C})$ and $M \in M_2(\mathbb{C})$ we have

$$\begin{aligned}\Phi(N\otimes M) &= \sum_{i,j\in\{0,1\}} K_{ij}(N\otimes M)K_{ij}^{\dagger} \\ &= \sum_{i,j\in\{0,1\}} (\langle i|\langle j|N|i\rangle|j\rangle)\otimes M \\ &= tr(N)M.\end{aligned}$$

Then

$$\Phi(J(\boldsymbol{T})) = \sum_{0\le i,j\le d-1} \Phi\big(\boldsymbol{T}(|i\rangle\langle j|)\otimes|i\rangle\langle j|\big) = \sum_{0\le i,j\le d-1} tr\big(\boldsymbol{T}(|i\rangle\langle j|)\big)|i\rangle\langle j| = tr_1(J(\boldsymbol{T})).$$

Now if we take $B = \mathbb{I}_2$, then the condition

$$\Phi(J(\boldsymbol{T})) = \Phi(X) = B = \mathbb{I}_2$$

ensures that $\boldsymbol{T}$ is trace-preserving, by the result of (c). Moreover, the condition

$$J(\boldsymbol{T}) = X \ge 0$$

ensures that $\boldsymbol{T}$ is completely positive, by the resulte of problem 4. Then finally, we can obtain the optimal success probability of attack based on CPTP map by solving the primal problem

$$\begin{aligned}\alpha = \max_{X}\ & tr(\frac{1}{4}QX) \\ s.t.\ \ & \Phi(X) = \mathbb{I}_2, \\ & X \ge 0,\end{aligned}$$

with the optimal success probability equal to α and the optimal CPTP map $\boldsymbol{T^*} = J^{-1}(X^*)$. The dual problem is

$$\begin{aligned}\beta = \min_{Y}\ & tr(Y) \\ s.t.\ \ & \Phi^*(Y) \ge \frac{1}{4}Q, \\ & Y = Y^{\dagger}.\end{aligned}$$

Notice that

$$\Phi^*(Y) = \sum_{i,j\in\{0,1\}} K_{ij}^{\dagger} Y K_{ij} = \sum_{i,j\in\{0,1\}} (|i\rangle|j\rangle\langle i|\langle j|)\otimes Y = \mathbb{I}_4\otimes Y,$$

the dual problem can have a more explicit form

$$\begin{aligned}\beta = \min_{Y}\ & tr(Y) \\ s.t.\ \ & \mathbb{I}_4\otimes Y \ge \frac{1}{4}Q, \\ & Y = Y^{\dagger}.\end{aligned}$$

(e) Let's solve the primal problem in (d):

$$\begin{aligned}\alpha = \max_X \ & tr(AX)\\ s.t. \quad & \Phi(X) = \mathbb{I}_2,\\ & X \geq 0.\end{aligned}$$

For Wiesner's scheme, we have

$$A = \frac{1}{4}Q = \frac{1}{4}\big(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3| + |\psi_4\rangle\langle\psi_4|\big),$$

where

$$|\psi_1\rangle = |0\rangle|0\rangle|0\rangle, \quad |\psi_2\rangle = |1\rangle|1\rangle|1\rangle, \quad |\psi_3\rangle = |+\rangle|+\rangle|+\rangle, \quad |\psi_2\rangle|-\rangle|-\rangle|-\rangle.$$

With help of matlab, we can easily find the eigenvalue decomposition of Q,

$$Q = U\Lambda U^\dagger,$$

where U is unitary, and

$$\Lambda = \text{diag}(\frac{3}{8}, \frac{3}{8}, \frac{1}{8}, \frac{1}{8}, 0, 0, 0, 0).$$

That is, all eigenvalues of A are

$$\lambda_1 = \lambda_2 = \frac{3}{8}, \quad \lambda_3 = \lambda_4 = \frac{1}{8}, \quad \lambda_5 = \lambda_6 = \lambda_7 = \lambda_8 = 0.$$

Then we can immediately obtain a upperbound for our objective function given that X is a feasible solution,

$$tr(AX) = tr(U\Lambda U^\dagger X) = tr(\Lambda U^\dagger XU) \leq \lambda_1(A)tr(U^\dagger XU) = \lambda_1(A)tr(X) = 2\lambda_1(A) = \frac{3}{4}.$$

Therefore if we can achieve this upperbound with some feasible X, then the problem is solved. Indeed, to make the inequality to become equality in the formula above, i.e.

$$tr(\Lambda U^\dagger XU) = \lambda_1(A)tr(U^\dagger XU),$$

we need the diagonal entries of $U^\dagger XU$ to focus on the first two entries which are associated with $\lambda_1(A), \lambda_2(A)$. Recall that $tr(U^\dagger XU) = tr(X) = 2$, a narutal guess would be

$$U^\dagger X^* U = \text{diag}(1, 1, 0, 0, 0, 0, 0, 0),$$

and we have

$$X^* = U\text{diag}(1, 1, 0, 0, 0, 0, 0, 0)U^\dagger = \begin{pmatrix} 3/4 & 0 & 0 & 1/4 & 0 & 1/4 & 1/4 & 0 \\ 0 & 1/12 & 1/12 & 0 & 1/12 & 0 & 0 & 1/12 \\ 0 & 1/12 & 1/12 & 0 & 1/12 & 0 & 0 & 1/12 \\ 1/4 & 0 & 0 & 1/12 & 0 & 1/12 & 1/12 & 0 \\ 0 & 1/12 & 1/12 & 0 & 1/12 & 0 & 0 & 1/12 \\ 1/4 & 0 & 0 & 1/12 & 0 & 1/12 & 1/12 & 0 \\ 1/4 & 0 & 0 & 1/12 & 0 & 1/12 & 1/12 & 0 \\ 0 & 1/4 & 1/4 & 0 & 1/4 & 0 & 0 & 3/4 \end{pmatrix}$$

$$= |\zeta_1\rangle\langle\zeta_1| + |\zeta_2\rangle\langle\zeta_2|,$$

where $|\zeta_1\rangle, |\zeta_2\rangle$ are the eigenstates of A corresponding to eigenvalues λ_1, λ_2,

$$|\zeta_1\rangle = \frac{1}{\sqrt{12}}(3,0,0,1,0,1,1,0)^\dagger = \frac{1}{\sqrt{12}}\big(3|0\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle\big),$$

$$|\zeta_2\rangle = \frac{1}{\sqrt{12}}(0,1,1,0,1,0,0,3)^\dagger = \frac{1}{\sqrt{12}}\big(|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle + 3|1\rangle|1\rangle|1\rangle\big).$$

It's easy chech that X^* is a feasible solution, i.e.

$$\Phi(X^*) = \mathbb{I}_2, \quad X^* \geq 0,$$

thus we have $\alpha = \frac{3}{4}$, the optimal success probability is $\frac{3}{4}$.

Our next mission is to recover $\boldsymbol{T}^*$ from X^*. Now we can make use of the useful results in problem 4. Let

$$Z_1 = \frac{1}{\sqrt{12}}\big(3|0\rangle|0\rangle\langle 0| + |0\rangle|1\rangle\langle 1| + |1\rangle|0\rangle\langle 1| + |1\rangle|1\rangle\langle 0|\big),$$

$$Z_2 = \frac{1}{\sqrt{12}}\big(|0\rangle|0\rangle\langle 1| + |0\rangle|1\rangle\langle 0| + |1\rangle|0\rangle\langle 0| + 3|1\rangle|1\rangle\langle 1|\big),$$

then we have

$$\boldsymbol{vec}(Z_1) = |\zeta_1\rangle, \quad \boldsymbol{vec}(Z_2) = |\zeta_2\rangle.$$

Define

$$\boldsymbol{T}_1(\rho) = Z_1\rho Z_1^\dagger, \quad \forall \rho \in M_2(\mathbb{C}),$$
$$\boldsymbol{T}_2(\rho) = Z_2\rho Z_2^\dagger, \quad \forall \rho \in M_2(\mathbb{C}).$$

By the result of problem 4(d), we have

$$J^{-1}(|\zeta_1\rangle\langle\zeta_1|) = \boldsymbol{T}_1, \quad J^{-1}(|\zeta_2\rangle\langle\zeta_2|) = \boldsymbol{T}_2.$$

Finally we have

$$\boldsymbol{T}^* = J^{-1}(X^*) = J^{-1}(|\zeta_1\rangle\langle\zeta_1|) + J^{-1}(|\zeta_2\rangle\langle\zeta_2|) = \boldsymbol{T}_1 + \boldsymbol{T}_2,$$

that is we have

$$\boldsymbol{T}^*(\rho) = Z_1\rho Z_1^\dagger + Z_2\rho Z_2^\dagger \quad \forall \rho \in M_2(\mathbb{C}).$$

(f) Consider a linear map U such that

$$U: \quad |0\rangle|0\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{12}}\Big(\big(3|0\rangle|0\rangle + |1\rangle|1\rangle\big) \otimes |0\rangle + \big(|0\rangle|1\rangle + |1\rangle|0\rangle\big) \otimes |1\rangle\Big),$$

$$U: \quad |1\rangle|0\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{12}}\Big(\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big) \otimes |0\rangle + \big(|0\rangle|0\rangle + 3|1\rangle|1\rangle\big) \otimes |1\rangle\Big).$$

By direct calculation, we can check that

$$\big|U|0\rangle|0\rangle|0\rangle\big| = \big|U|1\rangle|0\rangle|0\rangle\big| = 1, \quad (U|0\rangle|0\rangle|0\rangle)^\dagger(U|1\rangle|0\rangle|0\rangle) = 0,$$

therefore we can extend U to be a unitary operator for all three-qubits (use a similar argument for HW2 problem 6(b)). We still denote this extended unitary operator as U. Notice that

$$Z_1|0\rangle = \frac{1}{\sqrt{12}}\big(3|0\rangle|0\rangle + |1\rangle|1\rangle\big), \quad Z_1|1\rangle = \frac{1}{\sqrt{12}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big),$$

$$Z_2|0\rangle = \frac{1}{\sqrt{12}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big), \quad Z_2|1\rangle = \frac{1}{\sqrt{12}}\big(|0\rangle|0\rangle + 3|1\rangle|1\rangle\big),$$

thus we have

$$\begin{aligned} U(|0\rangle|0\rangle|0\rangle) &= (Z_1|0\rangle) \otimes |0\rangle + (Z_2|0\rangle) \otimes |1\rangle, \\ U(|1\rangle|0\rangle|0\rangle) &= (Z_1|1\rangle) \otimes |0\rangle + (Z_2|1\rangle) \otimes |1\rangle. \end{aligned}$$

Then for any single qubit $|\phi\rangle$, by linearity, we always have

$$U(|\phi\rangle|0\rangle|0\rangle) = (Z_1|\phi\rangle) \otimes |0\rangle + (Z_2|\phi\rangle) \otimes |1\rangle.$$

Notice that we have

$$\begin{aligned} tr_3(U|\phi\rangle|0\rangle|0\rangle\langle\phi|\langle 0|\langle 0|U^\dagger) &= tr_3\Big(Z_1|\phi\rangle\langle\phi|Z_1^\dagger \otimes |0\rangle\langle 0| + Z_2|\phi\rangle\langle\phi|Z_2^\dagger \otimes |1\rangle\langle 1| \\ &\qquad + Z_1|\phi\rangle\langle\phi|Z_2^\dagger \otimes |0\rangle\langle 1| + Z_2|\phi\rangle\langle\phi|Z_1^\dagger \otimes |1\rangle\langle 0|\Big) \\ &= Z_1|\phi\rangle\langle\phi|Z_1^\dagger + Z_2|\phi\rangle\langle\phi|Z_2^\dagger \\ &= \boldsymbol{T}^*(|\phi\rangle\langle\phi|). \end{aligned}$$

Now we can clarify our optimal attack found in (e). Given a money qubit $|\phi\rangle$, the attack steps are

(i) **Operation**: Append $|0\rangle|0\rangle$ to $|\phi\rangle$. **Outcome**: $|\phi\rangle|0\rangle|0\rangle$.

(ii) **Operation**: Apply U to $|\phi\rangle|0\rangle|0\rangle$. **Outcome**: $(Z_1|\phi\rangle) \otimes |0\rangle + (Z_2|\phi\rangle) \otimes |1\rangle$.

(iii) **Operation**: Trace out the third qubit. **Outcome**: $\boldsymbol{T}^*(|\phi\rangle\langle\phi|)$.