CS/Ph120 Homework 2 Solutions

October 25, 2016

Problem 1: Classical one-time pad

Solution: (Due to Daniel Gu)

1. Let X be the random variable which is the number of bits that Alice uses in total, and X_i be the number of bits that Alice uses at step i in the protocol. Then $X = \sum_{i=1}^{n} X_i$ and so by linearity of expectation

$$\mathbb{E}[X] = \mathbb{E}[\sum_{i=1}^{n} X_i] = \sum_{i=1}^{n} \mathbb{E}[X_i] = \frac{n}{2}$$

2. The scheme is certainly not correct: since Alice doesn't send her random choices (random bits) to Bob but only the ciphertext c, Bob has no idea which bits got XOR'd with the key and which got XOR'd with a random bit. No deterministic algorithm can decrypt the ciphertext accurately, since once we fix the ciphertext, key, and DEC(k, c), we can choose our random bits such that our message does not match our decryption algorithm's answer.

   However, the scheme is secure. The probability that the ith bit of the message is 0 (over the random choices made by Alice and a uniformly random key distribution) given that the ith bit of the ciphertext is b is $1/2$, since with probability $1/2$ we XOR b with the ith bit of the key, which without knowledge of the key is equally likely to be 0 or 1, so it has a $1/2$ chance of being b and producing 0, and with probability $1/2$ we XOR it with a uniformly random bit, which is also has a $1/2$ chance of being b. So given the ciphertext, the distribution of possible messages is the uniform distribution over all n bit messages, so the scheme is secure.

Problem 2: Superpositions and mixtures

Solution: (Due to Alex Meiburg)

(a)

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$$

(b) Note that $\rho_0 = \frac{1}{2}\mathbb{I}$. The probability for any given state is given by

$$\langle\psi|\rho_0|\psi|\psi|\rho_0|\psi\rangle = \left\langle \psi|\frac{1}{2}\mathbb{I}|\psi\middle|\psi|\frac{1}{2}\mathbb{I}|\psi\right\rangle = \frac{1}{2}\langle\psi|\psi|\psi|\psi\rangle = \frac{1}{2}$$

So that each measurement of a state gives a 50% probability of that occuring.
(c)

$$\rho_0 = |+\rangle \langle +| = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

$$\langle 0|\rho_0|0|0|\rho_0|0\rangle = \frac{1}{2}, \quad \langle 1|\rho_0|1|1|\rho_0|1\rangle = \frac{1}{2}$$

$$\langle +|\rho_0|+|+|\rho_0|+\rangle = \langle +|+|+|+\rangle \langle +|+|+|+\rangle = 1, \quad \langle -|\rho_0|-|-|\rho_0|-\rangle = \langle -|+|-|+\rangle \langle +|-|+|-\rangle = 0$$

So that in the standard basis it is completely random, while in the Hadamard basis it is guaranteed $|+\rangle$.

Problem 3: Quantum one-time pad

Solution: (Due to Anish Thilagar)

1. This protocol is correct. Bob will receive the state $H^k |\psi\rangle$. He can then apply H^k again, to get the qubit $H^{2k} |\psi\rangle = |\psi\rangle$ because $H^{2k} = (H^2)^k = I^k = I$. Therefore, he can correctly extract the message from Alice.

2. This protocol is not secure. Take the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |+\rangle)$. Under the action of H, this is an eigenvector with eigenvalue 1, so it will remain unchanged. Therefore, the ciphertext c will be equal to the message $m = |\psi\rangle$, so $p(|\psi\rangle\,|c) = 1 \neq p(|\psi\rangle) < 1$. Therefore, this protocol is not secure.

Problem 4: Unambiguous quantum state discrimination

Solution: (Due to Mandy Huo)

(a) If Alice measures in the standard basis then given that the state is $|0\rangle$ she will always get $|0\rangle$ so she will never misidentify it and given that the state is $|+\rangle$ she will get $|0\rangle$ half the time so she will misidentify it probability 1/2.

(b) If Alice measures in the Hadamard basis then given that the state is $|+\rangle$ she will always get $|+\rangle$ so she will never misidentify it. Given that the state is $|0\rangle$ she will get $|+\rangle$ half the time so she will misidentify it probability 1/2.

(c) Assuming both states are equally likely a priori, Alice can do better overall if she measures in the basis $\{|b_1\rangle, |b_2\rangle\}$ where $|b_1\rangle = \sin\frac{3\pi}{8}|0\rangle - \cos\frac{3\pi}{8}|1\rangle$ and $|b_2\rangle = \cos\frac{3\pi}{8}|0\rangle + \sin\frac{3\pi}{8}|1\rangle$, and identifies $|0\rangle$ when she gets the outcome $|b_1\rangle$ and $|+\rangle$ when she gets the outcome $|b_2\rangle$. Then the total probability of misidentifying is

$$
\begin{aligned}
\frac{1}{2}|\langle b_2|0\rangle|^2 + \frac{1}{2}|\langle b_1|+\rangle|^2 &= \frac{1}{2}\cos^2\frac{3\pi}{8} + \frac{1}{2}\frac{1}{2}\left(\sin^2\frac{3\pi}{8} + \cos^2\frac{3\pi}{8} - 2\sin\frac{3\pi}{8}\cos\frac{3\pi}{8}\right) \\
&= \frac{1}{2}\cos^2\frac{3\pi}{8} + \frac{1}{2}\frac{1}{2}\left(1 - \sin\frac{3\pi}{4}\right) \\
&= \frac{1}{2}\cos^2\frac{3\pi}{8} + \frac{1}{2}\frac{1}{2}\left(1 + \cos\frac{3\pi}{4}\right) \\
&= \cos^2\frac{3\pi}{8} = 0.15
\end{aligned}
$$

which is less than $\frac{1}{2}\frac{1}{2} = \frac{1}{4}$ in parts (a) and (b).

(d) If the state is $|+\rangle$ then Alice will get outcomes 2 and 3 with probabilities

$$
\begin{aligned}
\mathrm{tr}\{E_2|+\rangle\langle+|\} &= \mathrm{tr}\left\{\left(\frac{\sqrt{2}}{1+\sqrt{2}}|-\rangle\langle-|\right)|+\rangle\langle+|\right\} = 0, \\
\mathrm{tr}\{E_3|+\rangle\langle+|\} &= 1 - \mathrm{tr}\{E_1|+\rangle\langle+|\} - \mathrm{tr}\{E_2|+\rangle\langle+|\} = 1 - \frac{1}{\sqrt{2}(1+\sqrt{2})} = \frac{1}{\sqrt{2}}.
\end{aligned}
$$

So given that the state is $|+\rangle$, Alice will never misidentify the state and will fail to make an identification with probability $1/\sqrt{2}$.

If the state is $|0\rangle$ then Alice will get outcomes 1 and 3 with probabilities

$$
\begin{aligned}
&\mathrm{tr}\{E_1|0\rangle\langle 0|\} = 0, \\
&\mathrm{tr}\{E_3|0\rangle\langle 0|\} = 1 - \mathrm{tr}\{E_1|0\rangle\langle 0|\} - \mathrm{tr}\{E_2|0\rangle\langle 0|\} = 1 - \frac{\sqrt{2}}{2(1+\sqrt{2})} = \frac{1}{\sqrt{2}}.
\end{aligned}
$$

So given that the state is $|+\rangle$, Alice will never misidentify the state and will fail to make an identification with probability $1/\sqrt{2}$.

(e) There is no POVM that increases the chances of making a correct identification without increasing the chance of making an incorrect identification.

First we will show that any POVM such that the probability of mis-identification is zero must have the form $E_1 = \alpha|1\rangle\langle 1|$ and $E_2 = \beta|-\rangle\langle -|$, α, $\beta > 0$. Since we must have $\mathrm{tr}\{E_1|0\rangle\langle 0|\} = \langle 0|E_1|0\rangle = 0$ for zero chance of mis-identification in the $|0\rangle$ case, we have that either $|0\rangle$ is in the nullspace of E_1 or E_1 projects $|0\rangle$ onto $|1\rangle$. In the second case, we would have $E_1 = \alpha|1\rangle\langle 0|$, which is not Hermitian and thus not positive so E_1 must map $|0\rangle$ to the zero vector. Then E_1 has rank 1 so it has the form $E_1 = \alpha|b\rangle\langle 1|$. Then since E_1 must be positive (and thus Hermitian) we have $E_1 = \alpha|1\rangle\langle 1|$, $\alpha > 0$ (note if $E_1 = 0$ then Alice will always fail to make an identification in the $|+\rangle$ case.) Similarly, $\mathrm{tr}\{E_2|+\rangle\langle+|\} = \langle +|E_2|+\rangle = 0$ implies that $|+\rangle$ is either in the nullspace of E_2 or is projected onto $|-\rangle$, but the second case results in E_2 not positive semidefinite so we must have $E_2 = \beta|-\rangle\langle-|$, $\beta > 0$.

Then $E_3 = I - E_1 - E_2$ as before so that $\sum_i E_i = I$. What is left to check is whether E_3 is positive semidefinite. Since E_3 is given by

$$\begin{vmatrix} (1-\lambda) - \beta/2 & \beta/2 \\ \beta/2 & (1-\lambda) - a - \beta/2 \end{vmatrix} = \lambda^2 + (\alpha+\beta-2)\lambda - \left(\alpha + \beta - \frac{\alpha\beta}{2} - 1\right) = 0$$

so the eigenvalues are

$$\lambda = \frac{-(\alpha+\beta-2) \pm \sqrt{(\alpha+\beta-2)^2 + 4\left(\alpha+\beta-\frac{\alpha\beta}{2}-1\right)}}{2} = \frac{-(\alpha+\beta-2) \pm \sqrt{\alpha^2+\beta^2}}{2}.$$

Since we want a POVM that fails to make an identification with smaller probability, we need $\mathrm{tr}\{E_3|0\rangle\langle 0|\} = 1 - \frac{\beta}{2} < \frac{1}{\sqrt{2}}$ and $\mathrm{tr}\{E_3|+\rangle\langle+|\} = 1 - \frac{\alpha}{2} < \frac{1}{\sqrt{2}}$, that is,

$$\alpha > 2\left(\frac{\sqrt{2}-1}{\sqrt{2}}\right), \quad \beta > 2\left(\frac{\sqrt{2}-1}{\sqrt{2}}\right).$$

Then we have

$$-(\alpha+\beta-2) < 2 - 4\frac{\sqrt{2}-1}{\sqrt{2}} = -2 + \frac{4}{\sqrt{2}} = 2(\sqrt{2}-2 = 2\left(\sqrt{2}-1\right)$$

$$\sqrt{a^2+b^2} > \sqrt{2\left(2\frac{\sqrt{2}-1}{\sqrt{2}}\right)^2} = 2(\sqrt{2}-2 = 2\left(\sqrt{2}-1\right) > 0$$

so $\sqrt{a^2+b^2} > -(\alpha+\beta-2)$ and so E_3 will have one negative eigenvalue and thus is not positive. Hence there is no POVM that gives Alice a better chance of making a correct identification without increasing the change of making an incorrect identification.

Problem 5: Robustness of GHZ and W states

Solution: (Due to Mandy Huo)

(a) (i) Since $\mathrm{Tr}(|i\rangle\langle j|) = \langle j|i\rangle$ is 0 for $i \neq j$ and 1 for $i = j$, we have $\mathrm{Tr}_3(|GHZ_3\rangle\langle GHZ_3|) = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$, and so

$$\begin{aligned}\mathrm{Tr}(|GHZ_2\rangle\langle GHZ_2|\mathrm{Tr}_3(|GHZ_3\rangle\langle GHZ_3|)) &= \frac{1}{4}\mathrm{Tr}[(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)(|00\rangle\langle 00| + |11\rangle\langle 11|)] \\ &= \frac{1}{4}\mathrm{Tr}[(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)] \\ &= \frac{1}{2}\end{aligned}$$

(ii) Note that $\text{Tr}_3(|W_3\rangle\langle W_3|) = \frac{1}{3}(|10\rangle\langle 10| + |01\rangle\langle 01| + |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10|)$ so we have

$$\begin{aligned}\text{Tr}(|W_2\rangle\langle W_2|\text{Tr}_3(|W_3\rangle\langle W_3|)) &= \frac{1}{6}\text{Tr}[(|10\rangle + |01\rangle)(2\langle 10| + 2\langle 01|)] \\ &= \frac{2}{3}\end{aligned}$$

(b) (i) We have $\text{Tr}_3(|GHZ_N\rangle\langle GHZ_N|) = \frac{1}{2}(|0\rangle^{\otimes N-1}\langle 0|^{\otimes N-1} + |1\rangle^{\otimes N-1}\langle 1|^{\otimes N-1})$ so

$$\langle GHZ_N - 1|\text{Tr}_N(|GHZ_N\rangle\langle GHZ_N|) = \frac{1}{2}\langle GHZ_N - 1|$$

and thus

$$\begin{aligned}&\text{Tr}(|GHZ_{N-1}\rangle\langle GHZ_{N-1}|\text{Tr}_3(|GHZ_N\rangle\langle GHZ_N|)) \\ &\qquad = \frac{1}{4}\text{Tr}(|0\rangle^{\otimes N-1} + |1\rangle^{\otimes N-1})(\langle 0|^{\otimes N-1} + \langle 1|^{\otimes N-1}) \\ &\qquad = \frac{1}{2}\end{aligned}$$

(ii) We have $\langle W_{N-1}|\text{Tr}_N(|W_N\rangle\langle W_N|) = \frac{N-1}{N}\langle W_{N-1}|$ so

$$\begin{aligned}&\text{Tr}(|W_{N-1}\rangle\langle W_{N-1}|\text{Tr}_3(|W_N\rangle\langle W_N|)) \\ &\quad = \frac{1}{N}\text{Tr}(|10\ldots 0\rangle + |010\ldots 0\rangle + \cdots + |0\ldots 01\rangle)(\langle 10\ldots 0| + \langle 010\ldots 0| + \cdots + \langle 0\ldots 01|) \\ &\quad = \frac{N-1}{N}.\end{aligned}$$

Since $\dfrac{N-1}{N} > \dfrac{1}{2}$ for $N > 2$ the overlap between the N-qubit W states is greater than between the N-qubit GHZ states so we can conclude that the W states are more "robust" to tracing out a qubit.

Problem 6: Universal Cloning

Solution: (Due to De Huang)

(a) (i) We can see ρ and $T_1(\rho)$ as matrices in $C^{2\times 2}$ and $C^{4\times 4}$. Then we have

$$\begin{aligned}
T_1(\rho) &= \rho \otimes \frac{\mathbb{I}}{2} \\
&= \frac{1}{2}\begin{pmatrix} \rho_{11} & 0 & \rho_{12} & 0 \\ 0 & \rho_{11} & 0 & \rho_{12} \\ \rho_{21} & 0 & \rho_{22} & 0 \\ 0 & \rho_{21} & 0 & \rho_{22} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
&\quad + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
&= A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger,
\end{aligned}$$

where

$$A_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

It's easy to check that

$$A_1^\dagger A_1 + A_2^\dagger A_2 = \mathbb{I}.$$

Therefore T_1 is CPTP.

Indeed we can check that for any single qubit $|\psi\rangle$,

$$A_1|\psi\rangle = \frac{1}{\sqrt{2}}|\psi\rangle \otimes |0\rangle, \quad A_2|\psi\rangle = \frac{1}{\sqrt{2}}|\psi\rangle \otimes |1\rangle,$$

$$A_1^\dagger(|\psi\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}|\psi\rangle, \quad A_2^\dagger(|\psi\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}|\psi\rangle,$$

therefore

$$\begin{aligned}
A_1|\psi\rangle\langle\psi|A_1^\dagger + A_2|\psi\rangle\langle\psi|A_2^\dagger &= \frac{1}{2}|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| + \frac{1}{2}|\psi\rangle\langle\psi| \otimes |1\rangle\langle 1| \\
&= |\psi\rangle\langle\psi| \otimes \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\
&= |\psi\rangle\langle\psi| \otimes \frac{\mathbb{I}}{2} \\
&= T_1(|\psi\rangle\langle\psi|),
\end{aligned}$$

and

$$(A_1^\dagger A_1 + A_2^\dagger A_2)|\psi\rangle = \frac{1}{\sqrt{2}}A_1^\dagger(|\psi\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}A_2^\dagger(|\psi\rangle \otimes |1\rangle) = |\psi\rangle,$$

which again verifies our proof of CPTP.

The cloned qubit has density matrix $\frac{\mathbb{I}}{2}$, which actually carries no information. No matter what basis we use to measure the cloned qubit, we always get fair probability $\frac{1}{2}$ on both results. In the meanwhile, the first qubit is still in state $|\psi\rangle$.

(ii) Since $T_1(|\psi\rangle\langle\psi|) \geq 0$, we have

$$\begin{aligned}\big|\langle\psi|\langle\psi|T_1(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle\big| &= \langle\psi|\langle\psi|T_1(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle \\ &= \langle\psi|\langle\psi|\big(|\psi\rangle\langle\psi|\otimes\frac{\mathbb{I}}{2}\big)|\psi\rangle|\psi\rangle \\ &= \langle\psi||\psi\rangle\langle\psi||\psi\rangle \times \langle\psi|\frac{\mathbb{I}}{2}|\psi\rangle \\ &= \frac{1}{2}.\end{aligned}$$

(b) (i) Since $|0\rangle|0\rangle|0\rangle$ and $|1\rangle|0\rangle|0\rangle$ are orthogonal, we only need to verify that $U|0\rangle|0\rangle|0\rangle$ and $U|1\rangle|0\rangle|0\rangle$ are orthogonal.

Indeed, note that $|0\rangle|0\rangle|0\rangle, |0\rangle|0\rangle|1\rangle, |0\rangle|1\rangle|0\rangle, |0\rangle|1\rangle|1\rangle, |1\rangle|0\rangle|0\rangle, |1\rangle|0\rangle|1\rangle, |1\rangle|1\rangle|0\rangle, |1\rangle|1\rangle|1\rangle$ are orthogonal to each other, since

$$U|1\rangle|0\rangle|0\rangle = \sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}|1\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}|0\rangle|1\rangle|0\rangle,$$

we have

$$\langle 0|\langle 0|\langle 0|U|1\rangle|0\rangle|0\rangle = \langle 0|\langle 1|\langle 1|U|1\rangle|0\rangle|0\rangle = \langle 1|\langle 0|\langle 1|U|1\rangle|0\rangle|0\rangle = 0.$$

And since

$$U|0\rangle|0\rangle|0\rangle = \sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}|0\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}|1\rangle|0\rangle|1\rangle,$$

we immediately have that $U|0\rangle|0\rangle|0\rangle$ and $U|1\rangle|0\rangle|0\rangle$ are orthogonal.

Now we may extend $\{|0\rangle|0\rangle|0\rangle, |1\rangle|0\rangle|0\rangle\}$ to

$$\{|0\rangle|0\rangle|0\rangle, |1\rangle|0\rangle|0\rangle, \phi_3, \phi_4, \cdots, \phi_8\}$$

as an orthogonal basis of all three-qubits, and also extend $\{U|0\rangle|0\rangle|0\rangle, U|1\rangle|0\rangle|0\rangle\}$ to

$$\{U|0\rangle|0\rangle|0\rangle, U|1\rangle|0\rangle|0\rangle, \psi_3, \psi_4, \cdots, \psi_8\}$$

as another orthogonal basis of all three-qubits. Then one example of extending U to a valid three-qubit unitary $\widetilde{U}$ would be

$$\widetilde{U} : |0\rangle|0\rangle|0\rangle \to U|0\rangle|0\rangle|0\rangle, \quad \widetilde{U} : |1\rangle|0\rangle|0\rangle \to U|1\rangle|0\rangle|0\rangle,$$

$$\widetilde{U} : \phi_i \to \psi_i, \quad i = 3, 4, \cdots, 8.$$

It's easy to check that $\widetilde{U}$ is a valid three-qubit unitary because it linearly transforms an orthogonal basis to another orthogonal basis.

(ii) Let's define

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle).$$

For an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, we have

$$\begin{aligned}
U|\psi\rangle|0\rangle|0\rangle &= \alpha U|0\rangle|0\rangle|0\rangle + \beta U|1\rangle|0\rangle|0\rangle \\
&= \alpha\big(\sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}(|0\rangle|1\rangle + |1\rangle|0\rangle)|1\rangle\big) \\
&\quad + \beta\big(\sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}(|1\rangle|0\rangle + |0\rangle|1\rangle)|0\rangle\big) \\
&= \alpha\big(\sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{3}}|\Psi_+\rangle|1\rangle\big) + \beta\big(\sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{3}}|\Psi_+\rangle|0\rangle\big) \\
&= \big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)|0\rangle + \big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)|1\rangle,
\end{aligned}$$

$$\begin{aligned}
U|\psi\rangle|0\rangle|0\rangle\langle 0\langle 0\langle\psi|U^\dagger = &\big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\alpha}\sqrt{\frac{2}{3}}\langle 0|\langle 0| + \bar{\beta}\sqrt{\frac{1}{3}}\langle\Psi_+|\big) \otimes |0\rangle\langle 0| \\
&+ \big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\beta}\sqrt{\frac{2}{3}}\langle 1|\langle 1| + \bar{\alpha}\sqrt{\frac{1}{3}}\langle\Psi_+|\big) \otimes |1\rangle\langle 1| \\
&+ \big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\beta}\sqrt{\frac{2}{3}}\langle 1|\langle 1| + \bar{\alpha}\sqrt{\frac{1}{3}}\langle\Psi_+|\big) \otimes |0\rangle\langle 1| \\
&+ \big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\alpha}\sqrt{\frac{2}{3}}\langle 0|\langle 0| + \bar{\beta}\sqrt{\frac{1}{3}}\langle\Psi_+|\big) \otimes |1\rangle\langle 0|,
\end{aligned}$$

$$\begin{aligned}
T_2(|\psi\rangle\langle\psi|) = &\ \mathrm{tr}_3(U|\psi\rangle|0\rangle|0\rangle\langle 0\langle 0\langle\psi|U^\dagger) \\
= &\big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\alpha}\sqrt{\frac{2}{3}}\langle 0|\langle 0| + \bar{\beta}\sqrt{\frac{1}{3}}\langle\Psi_+|\big) \\
&+ \big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\beta}\sqrt{\frac{2}{3}}\langle 1|\langle 1| + \bar{\alpha}\sqrt{\frac{1}{3}}\langle\Psi_+|\big).
\end{aligned}$$

Then the success probability is

$$
\begin{aligned}
\big|\langle\psi|\langle\psi|T_2(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle\big| &= \Big|\langle\psi|\langle\psi|\big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\alpha}\sqrt{\frac{2}{3}}\langle 0|\langle 0| + \bar{\beta}\sqrt{\frac{1}{3}}\langle\Psi_+|\big)|\psi\rangle|\psi\rangle \\
&\quad + \langle\psi|\langle\psi|\big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big(\bar{\beta}\sqrt{\frac{2}{3}}\langle 1|\langle 1| + \bar{\alpha}\sqrt{\frac{1}{3}}\langle\Psi_+|\big)|\psi\rangle|\psi\rangle\Big| \\
&= \big|\langle\psi|\langle\psi|\big(\alpha\sqrt{\frac{2}{3}}|0\rangle|0\rangle + \beta\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big|^2 \\
&\quad + \big|\langle\psi|\langle\psi|\big(\beta\sqrt{\frac{2}{3}}|1\rangle|1\rangle + \alpha\sqrt{\frac{1}{3}}|\Psi_+\rangle\big)\big|^2 \\
&= \big||\alpha|^2\bar{\alpha}\sqrt{\frac{2}{3}} + |\beta|^2\bar{\alpha}\sqrt{\frac{2}{3}}\big|^2 + \big||\beta|^2\bar{\beta}\sqrt{\frac{2}{3}} + |\alpha|^2\bar{\beta}\sqrt{\frac{2}{3}}\big|^2 \\
&= \frac{2}{3}|\alpha|^2 + \frac{2}{3}|\beta|^2 \\
&= \frac{2}{3}.
\end{aligned}
$$

(c) (i) Note that

$$
P_+^\dagger = \mathbb{I}^\dagger - (|\Psi_-\rangle\langle\Psi_-|)^\dagger = \mathbb{I} - |\Psi_-\rangle\langle\Psi_-| = P_+,
$$

$$
\begin{aligned}
P_+P_+ &= (\mathbb{I} - |\Psi_-\rangle\langle\Psi_-|)(\mathbb{I} - |\Psi_-\rangle\langle\Psi_-|) \\
&= \mathbb{I} - 2|\Psi_-\rangle\langle\Psi_-| + |\Psi_-\rangle\langle\Psi_-||\Psi_-\rangle\langle\Psi_-| \\
&= \mathbb{I} - |\Psi_-\rangle\langle\Psi_-| \\
&= P_+.
\end{aligned}
$$

Then using the result of (a)(i), we have

$$
\begin{aligned}
T_3(\rho) &= \frac{2}{3}P_+(\rho\otimes\mathbb{I})P_+ \\
&= \frac{4}{3}P_+T_2(\rho)P_+ \\
&= \frac{4}{3}P_+(A_1\rho A_1^\dagger + A_2\rho A_2^\dagger)P_+^\dagger \\
&= (\frac{2}{\sqrt{3}}P_+A_1)\rho(\frac{2}{\sqrt{3}}P_+A_1)^\dagger + (\frac{2}{\sqrt{3}}P_+A_2)\rho(\frac{2}{\sqrt{3}}P_+A_2)^\dagger \\
&= V_1\rho V_1^\dagger + V_2\rho V_2^\dagger,
\end{aligned}
$$

where A_1, A_2 are defined in (a)(i), and

$$
V_1 = \frac{2}{\sqrt{3}}P_+A_1, \quad V_1 = \frac{2}{\sqrt{3}}P_+A_2.
$$

If we see $P_+ = \mathbb{I} - |\Psi_-\rangle\langle\Psi_-|$ as a matrix in $C^{4\times 4}$, then

$$
P_+ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
$$

By direct calculation, we can check that

$$\begin{aligned} V_1^\dagger V_1 + V_2^\dagger V_2 &= \frac{4}{3} A_1^\dagger P_+^\dagger P_+ A_1 + \frac{4}{3} A_2^\dagger P_+^\dagger P_+ A_2 \\ &= \frac{4}{3} A_1^\dagger P_+ A_1 + \frac{4}{3} A_2^\dagger P_+ A_2 \\ &= \mathbb{I}. \end{aligned}$$

Therefore T_3 is CPTP.

(ii) For any single-state $|\psi\rangle$, we have

$$\begin{aligned} \langle\psi|\langle\psi||\Psi_-\rangle &= \frac{1}{\sqrt{2}}(\langle\psi|0\rangle\langle\psi|1\rangle - \langle\psi|1\rangle\langle\psi|0\rangle) = 0, \\ \langle\psi|\langle\psi|P_+ &= \langle\psi|\langle\psi| - \langle\psi|\langle\psi||\Psi_-\rangle\langle|\Psi_-| = \langle\psi|\langle\psi|, \\ P_+|\psi\rangle|\psi\rangle &= |\psi\rangle|\psi\rangle - |\Psi_-\rangle\langle|\Psi_-||\psi\rangle|\psi\rangle = |\psi\rangle|\psi\rangle, \end{aligned}$$

thus the success probability of T_3 is

$$\begin{aligned} \big|\langle\psi|\langle\psi|T_3(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle\big| &= \frac{2}{3}\big|\langle\psi|\langle\psi|P_+(|\psi\rangle\langle\psi| \otimes \mathbb{I})P_+|\psi\rangle|\psi\rangle\big| \\ &= \frac{2}{3}\Big|\langle\psi|\langle\psi|(|\psi\rangle\langle\psi| \otimes \mathbb{I}))|\psi\rangle|\psi\rangle\Big| \\ &= \frac{2}{3}(\langle\psi||\psi\rangle\langle\psi||\psi\rangle)(\langle\psi|\mathbb{I}|\psi\rangle) \\ &= \frac{2}{3}. \end{aligned}$$

(iii) We can see that for any single-state $|\psi\rangle$,

$$\big|\langle\psi|\langle\psi|T_2(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle\big| = \big|\langle\psi|\langle\psi|T_3(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle\big| = \frac{2}{3},$$

that is, the map T_2 and T_3 have the same success probability. The essential reason for this result is that we actually have

$$T_2(|\psi\rangle\langle\psi|) = T_3(|\psi\rangle\langle\psi|)$$

for any single-state $|\psi\rangle$. To see this, we first rewrite $U|\psi\rangle|0\rangle|0\rangle$ as

$$\begin{aligned} U|\psi\rangle|0\rangle|0\rangle &= \alpha U|0\rangle|0\rangle|0\rangle + \beta U|1\rangle|0\rangle|0\rangle \\ &= \alpha\Big(\sqrt{\frac{2}{3}}|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{6}}(|0\rangle|1\rangle + |1\rangle|0\rangle)|1\rangle\Big) \\ &\quad + \beta\Big(\sqrt{\frac{2}{3}}|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{6}}(|1\rangle|0\rangle + |0\rangle|1\rangle)|0\rangle\Big) \\ &= \frac{1}{\sqrt{3}}|\Phi_+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{\sqrt{3}}|\Phi_-\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{\sqrt{3}}|\Psi_+\rangle(\alpha|1\rangle + \beta|0\rangle) \\ &= \frac{1}{\sqrt{3}}|\Phi_+\rangle|\psi\rangle + \frac{1}{\sqrt{3}}|\Phi_-\rangle(Z|\psi\rangle) + \frac{1}{\sqrt{3}}|\Psi_+\rangle(X|\psi\rangle). \end{aligned}$$

Here $|\Phi_+\rangle, |\Phi_-\rangle, |\Psi_+\rangle$ together with $|\Psi_-\rangle$ are the Bell basis, i.e.

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \quad |\Phi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle),$$

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle), \quad |\Psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle).$$

Then we have

$$\begin{aligned}
T_2(|\psi\rangle\langle\psi|) = &\ \mathrm{tr}_3(U|\psi\rangle|0\rangle|0\rangle\langle 0\langle 0\langle\psi|U^\dagger) \\
= &\ \frac{1}{3}\Big(\mathrm{tr}(|\psi\rangle\langle\psi|)|\Phi_+\rangle\langle\Phi_+| + \mathrm{tr}(Z|\psi\rangle\langle\psi|Z)|\Phi_-\rangle\langle\Phi_-| + \mathrm{tr}(X|\psi\rangle\langle\psi|X)|\Psi_+\rangle\langle\Psi_+| \\
&\quad + \mathrm{tr}(|\psi\rangle\langle\psi|Z)|\Phi_+\rangle\langle\Phi_-| + \mathrm{tr}(|\psi\rangle\langle\psi|X)|\Phi_+\rangle\langle\Psi_+| + \mathrm{tr}(Z|\psi\rangle\langle\psi|)|\Phi_-\rangle\langle\Phi_+| \\
&\quad + \mathrm{tr}(Z|\psi\rangle\langle\psi|X)|\Phi_-\rangle\langle\Psi_+| + \mathrm{tr}(X|\psi\rangle\langle\psi|)|\Psi_+\rangle\langle\Phi_+| + \mathrm{tr}(X|\psi\rangle\langle\psi|Z)|\Psi_+\rangle\langle\Phi_-|\Big) \\
= &\ \frac{1}{3}\Big(\langle\psi|\psi\rangle|\Phi_+\rangle\langle\Phi_+| + \langle\psi|\psi\rangle|\Phi_-\rangle\langle\Phi_-| + \langle\psi|\psi\rangle|\Psi_+\rangle\langle\Psi_+| \\
&\quad + \langle\psi|Z|\psi\rangle|\Phi_+\rangle\langle\Phi_-| + \langle\psi|X|\psi\rangle|\Phi_+\rangle\langle\Psi_+| + \langle\psi|Z|\psi\rangle|\Phi_-\rangle\langle\Phi_+| \\
&\quad + \langle\psi|XZ|\psi\rangle|\Phi_-\rangle\langle\Psi_+| + \langle\psi|X|\psi\rangle|\Psi_+\rangle\langle\Phi_+| + \langle\psi|ZX|\psi\rangle|\Psi_+\rangle\langle\Phi_-|\Big)
\end{aligned}$$

On the other hand, since

$$|\Phi_+\rangle\langle\Phi_+| + |\Phi_-\rangle\langle\Phi_-| + |\Psi_+\rangle\langle\Psi_+| + |\Psi_-\rangle\langle\Psi_-| = \mathbb{I},$$

we have

$$\mathbb{I} - |\Psi_-\rangle\langle\Psi_-| = |\Phi_+\rangle\langle\Phi_+| + |\Phi_-\rangle\langle\Phi_-| + |\Psi_+\rangle\langle\Psi_+|.$$

Thus

$$\begin{aligned}
&T_3(|\psi\rangle\langle\psi|) \\
= &\ \frac{2}{3}(\mathbb{I} - |\Psi_-\rangle\langle\Psi_-|)(|\psi\rangle\langle\psi| \otimes \mathbb{I})(\mathbb{I} - |\Psi_-\rangle\langle\Psi_-|) \\
= &\ \frac{2}{3}\big(|\Phi_+\rangle\langle\Phi_+| + |\Phi_-\rangle\langle\Phi_-| + |\Psi_+\rangle\langle\Psi_+|\big)(|\psi\rangle\langle\psi| \otimes \mathbb{I})\big(|\Phi_+\rangle\langle\Phi_+| + |\Phi_-\rangle\langle\Phi_-| + |\Psi_+\rangle\langle\Psi_+|\big) \\
= &\ \frac{2}{3}\Big(|\Phi_+\rangle\langle\Phi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_+\rangle\langle\Phi_+| + |\Phi_+\rangle\langle\Phi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_-\rangle\langle\Phi_-| \\
&\quad + |\Phi_+\rangle\langle\Phi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Psi_+\rangle\langle\Psi_+| + |\Phi_-\rangle\langle\Phi_-|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_+\rangle\langle\Phi_+| \\
&\quad + |\Phi_-\rangle\langle\Phi_-|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_-\rangle\langle\Phi_-| + |\Phi_-\rangle\langle\Phi_-|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Psi_+\rangle\langle\Psi_+| \\
&\quad + |\Psi_+\rangle\langle\Psi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_+\rangle\langle\Phi_+| + |\Psi_+\rangle\langle\Psi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_-\rangle\langle\Phi_-| \\
&\quad + |\Psi_+\rangle\langle\Psi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Psi_+\rangle\langle\Psi_+|\Big).
\end{aligned}$$

Note that

$$\langle\Phi_+|(|\psi\rangle\langle\psi| \otimes \mathbb{I})|\Phi_+\rangle = \frac{1}{2}\langle\psi|(|0\rangle\langle 0| + |1\rangle\langle 1|)|\psi\rangle = \frac{1}{2}\langle\psi|\psi\rangle,$$

$$\langle\Phi_-|(|\psi\rangle\langle\psi|\otimes\mathbb{I})|\Phi_-\rangle = \frac{1}{2}\langle\psi|(|0\rangle\langle 0| + |1\rangle\langle 1|)|\psi\rangle = \frac{1}{2}\langle\psi|\psi\rangle,$$

$$\langle\Psi_+|(|\psi\rangle\langle\psi|\otimes\mathbb{I})|\Psi_+\rangle = \frac{1}{2}\langle\psi|(|0\rangle\langle 0| + |1\rangle\langle 1|)|\psi\rangle = \frac{1}{2}\langle\psi|\psi\rangle,$$

$$\langle\Phi_+|(|\psi\rangle\langle\psi|\otimes\mathbb{I})|\Phi_-\rangle = \frac{1}{2}\langle\psi|(|0\rangle\langle 0| - |1\rangle\langle 1|)|\psi\rangle = \frac{1}{2}\langle\psi|Z|\psi\rangle,$$

$$\langle\Phi_+|(|\psi\rangle\langle\psi|\otimes\mathbb{I})|\Psi_+\rangle = \frac{1}{2}\langle\psi|(|0\rangle\langle 1| + |1\rangle\langle 0|)|\psi\rangle = \frac{1}{2}\langle\psi|X|\psi\rangle,$$

$$\langle\Phi_-|(|\psi\rangle\langle\psi|\otimes\mathbb{I})|\Psi_+\rangle = \frac{1}{2}\langle\psi|(|1\rangle\langle 0| - |0\rangle\langle 1|)|\psi\rangle = \frac{1}{2}\langle\psi|XZ|\psi\rangle.$$

Therefore

$$\begin{aligned} T_3(|\psi\rangle\langle\psi|) &= \frac{1}{3}\Big(\langle\psi|\psi\rangle|\Phi_+\rangle\langle\Phi_+| + \langle\psi|\psi\rangle|\Phi_-\rangle\langle\Phi_-| + \langle\psi|\psi\rangle|\Psi_+\rangle\langle\Psi_+| \\ &\quad + \langle\psi|Z|\psi\rangle|\Phi_+\rangle\langle\Phi_-| + \langle\psi|X|\psi\rangle|\Phi_+\rangle\langle\Psi_+| + \langle\psi|Z|\psi\rangle|\Phi_-\rangle\langle\Phi_+| \\ &\quad + \langle\psi|XZ|\psi\rangle|\Phi_-\rangle\langle\Psi_+| + \langle\psi|X|\psi\rangle|\Psi_+\rangle\langle\Phi_+| + \langle\psi|ZX|\psi\rangle|\Psi_+\rangle\langle\Phi_-|\Big) \\ &= T_2(|\psi\rangle\langle\psi|) \end{aligned}$$

It's done.