1 Question 1: Communication Using Qubits

(a) Suppose that we are given a device that can randomly generate any pure state with equal probability. Calculate the density matrix of the output state from this device.

Ans: $\rho = \frac{1}{2}\mathbb{I}_2$.

Solution:

[By Observation]
We parametrise the qubit state on a Bloch sphere. Notice that for any state $|\psi\rangle$ with Bloch vector $\vec{n}$, there is a corresponding state $|\varphi\rangle$ with Bloch vector $-\vec{n}$. Since a qubit state can be represented by

$$\rho = \frac{1}{2}(\mathbb{I} + \vec{n} \cdot \vec{\sigma})$$

where $\vec{\sigma}$ are the Pauli matrices, the sum of the density matrices of $|\psi\rangle$ and $|\varphi\rangle$ is simply

$$A = \mathbb{I}$$

Summing this value over all pure states with equal probability will yield $\mathbb{I}$ still, but since we double counted the states, the final density matrix is $\frac{1}{2}\mathbb{I}$.

[Proper Way]
We parametrise the qubit state on a Bloch sphere. For equal probability, the probability density function is $p(\Omega) = \frac{1}{4\pi}$, which gives $\int p(\Omega) d\Omega = 1$. A generic qubit state can be written as

$$\rho(\Omega) = \begin{bmatrix} \cos^2\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)e^{i\phi} \\ \cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right)e^{-i\phi} & \sin^2\left(\frac{\theta}{2}\right) \end{bmatrix}$$

The resulting density matrix is simply

$$\rho = \frac{1}{4\pi}\int_0^{\pi} d\theta \int_0^{2\pi} d\phi \rho(\Omega)$$

which gives $\rho = \frac{1}{2}\mathbb{I}_2$.

(b) Using the properties of a density matrix, prove that the Holevo quantity for any encoding on a n-dimensional quantum system is bounded by $\log_2 n$.

Furthermore, prove that this bound is tight.

Ans:

[Bound]
From properties of density matrix, we have that ρ has n eigenvalues λ_i that are non-negative and sum to 1. Hence, we can write the von-Neumann entropy as

$$S(\rho) = -\sum_i \lambda_i \log_2(\lambda_i)$$

We can maximise this with constraints $\sum_i \lambda_i = 1$ and $\lambda \geq 0$ by using Lagrange multipliers. The Lagrangian of this problem is

$$L = -\sum_i \lambda_i \log_2(\lambda_i) + \mu(\sum_i \lambda_i - 1) - \sum_i \nu_i(\lambda_i)$$

To maximise, we set $\frac{\partial L}{\partial \lambda_i} = 0$, and obtain

$$\lambda_i = 2^{-\frac{1}{\ln 2} + \mu + \nu_i}$$

This satisfies the positivity constraint for any ν_i and μ, and substituting the result into $\sum_i \lambda_i = 1$ yields

$$n 2^{-\frac{1}{\ln 2} + \mu + \nu_i} = 1$$

which can be simplified to get $\mu + \nu_i = \frac{1}{\ln 2} - \log_2 n$. This gives $\lambda_i = \frac{1}{n}$. Therefore, the maxima of $S(\rho)$ is $\log_2 n$. Therefore, since $\chi(\rho) \leq S(\rho)$, we have that the Holevo quantity is bounded by $\log_2 n$.

[Tightness]
$\rho_j = |j\rangle\langle j|$ with $\langle j|j'\rangle = \delta_{jj'}$ and $p_j = \frac{1}{n}$ satisfies the bound, hence, the bound is tight.

(c-i) List the unitaries that A can perform on her qubit in $|\psi^-\rangle_{AB}$ to obtain states $|\psi^-\rangle_A B$, $|\psi^+\rangle_A B$, $|\phi^+\rangle_A B$, and $|\phi^-\rangle_A B$. [Note: $|\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B)$, $|\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B)$, $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$]

Ans: $\mathbb{I}_2$, Z, X, XZ.

(ii) Propose a method for A to send the information of two classical bits if A and B begins with an entangled state $|\psi^-\rangle_{AB}$.

Ans: A encodes each message as a unitary from $\{\mathbb{I}, Z, X, XZ\}$ (i.e. If message is 00, encoding is $\mathbb{I}$, message is 01, encoding is Z etc). Based on the message, A performs the corresponding unitary and sends her qubit to B. When B receives the message, he measures the two qubits in the Bell basis to decode the message. [Note: This is superdense coding]

(d) Explain how B can obtain his desired bit k_j from m and the PR box.

Ans: B can first insert some b into the PR box to obtain some y. One can then XOR y and m to obtain

$$\begin{aligned} y \oplus m &= k_0 \oplus x \oplus y \\ &= k_0 \oplus ab \\ &= k_0 \oplus (k_0 \oplus k_1)b \end{aligned}$$

If $b = 0$, the XOR is k_0. If $b = 1$, the XOR is k_1. Hence, to get his desired bit k_j, B can simply insert $b = j$ to get $k_j = m \oplus y$.