ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 6

HS 12
Prof. R. Renner

Exercise 6.1 Data hiding

Suppose you have two agents, Alice and Bond, at your service. You want them to deliver a secret (classical) message to your ally Charlie. You will give Alice and Bond two different states (i.e. an encryption of your message), so that they cannot extract the secret message unless they are physically together. Specifically, data hiding is what you want: states that are easily distinguishable by doing a certain class of operations, such as a global measurement on Alice and Bond's systems together, but they are nearly indistinguishable under a different, restricted class of operations, such as local operations and classical communication (LOCC). Formally, we say that a family of states $\{\rho^i\}_i$ is ε-secure under a set of operations $\mathbb{E}$ if

$$\delta(\mathcal{E}(\rho^i), \mathcal{E}(\rho^j)) < \varepsilon, \quad \forall i, j, \quad \forall \mathcal{E} \in \mathbb{E}.$$

In this exercise we will consider a data hiding scheme which is secure under LOCC and so the original message can only be recovered if global measurements on the joint system are allowed. Consider a $2d$-qubit Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$, and the computational basis of both spaces. Consider the projectors onto the symmetric and antisymmetric subspaces of $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$\Pi^S = \frac{1}{2} \sum_{i<j} \Big(|i\rangle_A |j\rangle_B + |j\rangle_A |i\rangle_B \Big) \Big(\langle i|_A \langle j|_B + \langle j|_A \langle i|_B \Big) + \sum_i |i\rangle_A |i\rangle_B \langle i|_A \langle i|_B,$$
$$\Pi^A = \frac{1}{2} \sum_{i<j} \Big(|i\rangle_A |j\rangle_B - |j\rangle_A |i\rangle_B \Big) \Big(\langle i|_A \langle j|_B - \langle j|_A \langle i|_B \Big).$$

You will encode only one bit of information, b, giving Alice and Bond each their $d-$qubit part of ρ^b_{AB}, with

$$\rho^{b=0} = \frac{2}{d(d+1)} \Pi^S, \qquad \rho^{b=1} = \frac{2}{d(d-1)} \Pi^A.$$

a) Show that $\rho^{b=0}$ and $\rho^{b=1}$ are valid density operators and explain how you would proceed to recover b if you had access to Alice and Bond's systems (together).

b) Consider the flip operator in basis $\{|i\rangle_A |j\rangle_B\}_{ij}$,

$$F = \Pi^S - \Pi^A = \sum_{i,j} |i\rangle_A |j\rangle_B \langle j|_A \langle i|_B.$$

Show that, for all operators $M_A \in \mathrm{End}(\mathcal{H}_A), N_B \in \mathrm{End}(\mathcal{H}_B)$, $\mathrm{Tr}[F(M_A \otimes N_B)] = \mathrm{Tr}(M_A N_B)$. In particular, for all pure states $|x\rangle_A, |y\rangle_B$, $\mathrm{Tr}[F|xy\rangle\langle xy|] = |\langle x|y\rangle|^2$.

c) Suppose that Alice and Bond perform local projective measurements in arbitrary bases, $\{|x\rangle_A\}$ and $\{|y\rangle_B\}$ respectively. We denote the joint probability distribution of the outcomes P_{XY} when they measure state $\rho^{b=0}$ and Q_{XY} when they measure $\rho^{b=1}$. We want them to be unable to distinguish the two distributions, so we want to show that $\delta(P_{XY}, Q_{XY})$ is small. Remember that

$$P_{XY}(x,y) = \mathrm{Tr}(|xy\rangle\langle xy| \rho^{b=0}), \quad Q_{XY}(x,y) = \mathrm{Tr}(|xy\rangle\langle xy| \rho^{b=1}).$$

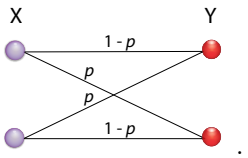
Use the results from *b*) to show that $\delta(P_{XY}, Q_{XY}) \leq \frac{2}{d+1}$.

Hint: Start from the trace distance as $\delta(P_{XY}, Q_{XY}) = \sum_{x,y \in \mathcal{S}} P_{XY}(x,y) - Q_{XY}(x,y)$, with $\mathcal{S} = \{(x,y) : P_{XY}(x,y) > Q_{XY}(x,y)\}$.

Exercise 6.2 Classical channels as trace-preserving completely positive maps.

You can represent classical channels as trace-preserving completely positive maps (CPTPMs).

a) Take the binary symmetric channel $\mathbf{p}$,



Recall that we can represent the probability distributions on both ends of the channel as quantum states in a given basis: for instance, if $P_X(0) = q, P_X(1) = 1 - q$, we may express this as the 1-qubit mixed state $\rho_X = q\ |0\rangle\langle 0| + (1-q)\ |1\rangle\langle 1|$.

What is the quantum state ρ_Y that represents the final probability distribution P_Y in the computational basis?

b) We can represent the channel as a map

$$\mathcal{E}_{\mathbf{p}} : \mathcal{S}(\mathcal{H}_X) \mapsto \mathcal{S}(\mathcal{H}_Y)$$
$$\rho_X \to \rho_Y.$$

An operator-sum representation (also called the Kraus-operator representation) of a CPTP map $\mathcal{E} : \mathcal{S}(\mathcal{H}_X) \to \mathcal{S}(\mathcal{H}_Y)$ is a decomposition $\{E_k\}_k$ of operators $E_k \in \mathrm{Hom}(\mathcal{H}_X, \mathcal{H}_Y)$, $\sum_k E_k {E_k}^\dagger = \mathbb{1}$, such that

$$\mathcal{E}(\rho_X) = \sum_k E_k \rho_X {E_k}^\dagger.$$

Find an operator-sum representation of $\mathcal{E}_{\mathbf{p}}$.

Hint: Think of each operator $E_k = E_{xy}$ as the representation of the branch that maps input x to output y.

c) Now we have a representation of the classical channel in terms of the evolution of a quantum state. What happens if the initial state ρ_X is not diagonal in the computational basis?

d) Consider an arbitrary classical channel $\mathbf{p}$ from an n-bit space X to an m-bit space Y, defined by the conditional probabilities $\left\{P_{Y|X=x}(y)\right\}_{xy}$.

Express $\mathbf{p}$ as a map $\mathcal{E}_{\mathbf{p}} : \mathcal{S}(\mathcal{H}_X) \to \mathcal{S}(\mathcal{H}_Y)$ in the operator-sum representation.

Exercise 6.3 CPTPMs as channels

In this exercise we will go the other way around: we are given a CPTPM and will find a way of expressing it as a channel, and compute its capacity.
Consider two single-qubit Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and a CPTPM

$$\mathcal{E}_p : \mathcal{S}(\mathcal{H}_X) \mapsto \mathcal{S}(\mathcal{H}_Y) \tag{D}$$
$$\rho \to p\frac{\mathbb{1}}{2} + (1-p)\rho.$$

a) Find an operator-sum representation for $\mathcal{E}_p$.

Hint: Remember that $\rho \in \mathcal{S}(\mathcal{H}_A)$ can be written in the Bloch sphere representation:

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma}), \quad \vec{r} \in \mathbb{R}^3, \quad |\vec{r}| \leq 1, \quad \vec{r}\cdot\vec{\sigma} = r_x\sigma_x + r_y\sigma_y + r_z\sigma_z, \tag{1}$$

where σ_x, σ_y and σ_z are Pauli matrices. It may be useful to show that

$$\mathbb{1} = \frac{1}{2}(\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z).$$

b) What happens to the Bloch radius $\vec{r}$ of the initial state when we apply $\mathcal{E}_p$? How can this be interpreted?

c) Now we will see what happens when we use this quantum channel to send classical information. We start with an arbitrary input probability distribution $P_X(0) = q, P_X(1) = 1 - q$. We encode this distribution in a state $\rho_X = q\ |0\rangle\langle 0| + (1-q)|1\rangle\langle 1|$. Now we send ρ_X over the quantum channel, i.e., we let it evolve under $\mathcal{E}_{\mathbf{p}}$. Finally, we measure the output state, $\rho_Y = \mathcal{E}_{\mathbf{p}}(\rho_X)$ in the computational basis.

Compute the conditional probabilities $\left\{P_{Y|X=x}(y)\right\}_{xy}$.

d) Maximise the mutual information over q to find the classical channel capacity of the depolarizing channel (D).

e) What happens to the channel capacity if we measure the final state in a different basis?