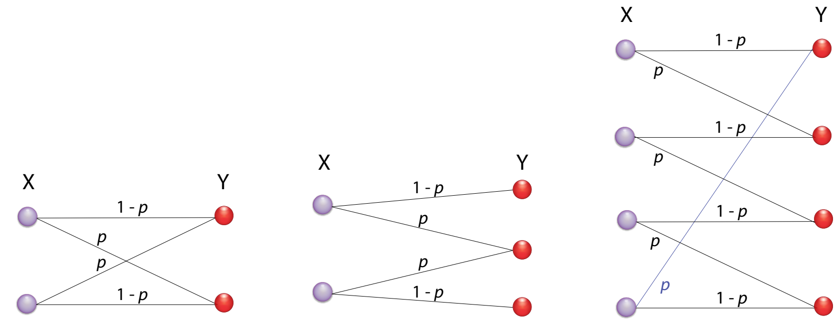
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 3

HS 12
Prof. R. Renner

Exercise 3.1 Channel capacity



(a) Binary Symmetric Channel

(b) Symmetric Erasure Channel

(c) Yet Another Channel

a) The asymptotic channel capacity is given by

$$C = \max_{P_X} I(X:Y).$$

Calculate the asymptotic capacities of the first two channels depicted above.

b) We can exploit the symmetries of some channels to simplify the calculation of the capacity.

Consider N possible probability distributions as input to a general channel, $\left\{P_X^i\right\}_i$, with the property that $I(X:Y)_{P^i} = I(X:Y)_{P^j}, \forall i,j$. Suppose you choose which distribution to use for the input by checking a random variable, B, with possible values $b = \{1,\dots,N\}$. Show that $I(X:Y|B) \leq I(X:Y)$.

How can you use that to find the probability distribution P_X that maximises the mutual information for symmetric channels? **Hint:** consider $\left\{P_X^i\right\}_i$ permutations of P_X^1.

c) Using the result from *b*), compute the capacity of the last channel. How would you proceed to reliably transmit one bit of information?

Exercise 3.2 Smooth min-entropy in the i.i.d. limit

The smooth min-entropy of a random variable X over $\mathcal{X}$ is defined as

$$H_{\min}^{\epsilon}(X)_P = \max_{Q_X \in \mathcal{B}^{\epsilon}(P_X)} H_{\min}(X)_Q, \tag{1}$$

where the maximum is taken over all probability distributions Q_X that are ϵ-close to P_X. Furthermore, we define an i.i.d. random variable $\vec{X} = \{X_1, X_2, \dots, X_n\}$ on $\mathcal{X}^{\times n}$ with $P_{\vec{X}}(\vec{x}) = \prod_{i=1}^n P_X(x_i)$.
Use the weak law of large numbers to show that the smooth min-entropy converges to the Shannon entropy $H(X)$ in the i.i.d. limit:

$$\lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} H_{\min}^{\epsilon}(\vec{X})_{P^n} = H(X)_P. \tag{2}$$

Exercise 3.3 Quantum-Telepathy Game: Introduction

a) Consider a game with two players, Alice (P_1) and Bob (P_2). They first agree on a strategy and then each receive one qubit of the quantum state:

$$|\phi\rangle = \frac{1}{\sqrt{2}} \left(|+-\rangle + |-+\rangle\right), \tag{3}$$

in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. The players cannot communicate once they get their qubits, and they must output two bits x_1 and x_2. They win if $x_1 \neq x_2$.

i) Find projective measurements that the players can perform so that they always get opposite outcomes x_1 and x_2.

ii) Explain how this game can be won without using $|\phi\rangle$.

b) Now we consider a game with 3 players. Initially, each player controls one qubit of the quantum state

$$|\Psi_-^3\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle). \tag{4}$$

Two of the three players, Alice (P_1) and Bob (P_2), will be chosen randomly and separated from the third player (and also each other) so that they cannot communicate. The third player, Charlie (P_3), will then perform a measurement on his qubit and will have one of two outcomes. Depending on the outcome, Charlie will choose a bit b to be either 0 or 1. He then forwards b to Alice and Bob. Finally Alice and Bob each output a bit: x_1 and x_2. They win if $x_1 \neq x_2$.

In order to use the quantum state they share to their advantage, Alice and Bob want to perform measurements (which dependend on the bit b they received) such that they get different outcomes.

i) First, rewrite the state $|\phi\rangle$ in the computational basis ($\{|0\rangle, |1\rangle\}$ for each qubit).

ii) What projective measurement should Charlie do so that when he gets outcome $b = 0$ the other two players are left with the state $|\phi\rangle$ from part (a) (Eqn. 3)? Note that if we project onto a state $|\tau\rangle$ on system 3, then the post-measurement state, given an initial pure state $|\Phi\rangle$, is given by:

$$\frac{\left(\mathbb{1}^{\otimes 2} \otimes \langle\tau|_3\right)|\Phi\rangle}{\left|\left(\mathbb{1}^{\otimes 2} \otimes \langle\tau|_3\right)|\Phi\rangle\right|},$$

where $\mathbb{1}$ is the identity operator on a qubit space.

iii) What is the state $|\psi\rangle$ that Alice and Bob share after Charlie gets the other outcome ($b = 1$)? Write $|\psi\rangle$ in the basis $\{|\circlearrowright\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}, |\circlearrowleft\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}\}$.

iv) What projective measurements should Alice and Bob do in order to get different results from the state $|\psi\rangle$?

Exercise 3.4 Quantum-Telepathy Game: The Full Story

Now we consider the full quantum-telepathy game. The game starts with n collaborating players $P_1, P_2, \ldots, P_n$ who each have a qubit of a large state $|\Psi\rangle$ in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ so player P_i has control of the qubit in the space $\mathcal{H}_i$. Then two of players, P_1 and P_2, will be randomly selected and separated from the other players. They are separated without the knowledge of which other player was selected, and they cannot communicate with any of the players, including each other. The remaining $n-2$ players are allowed to communicate with each other, and perform measurements on the qubits they each control. They then send a bit b (either 0 or 1) to the two separated players. P_1 and P_2 then output bits x_1 and x_2 respectively. They win the game if $x_1 \neq x_2$.
We know from the previous exercise that the game will always be won if the last three players share the state $|\Psi_-^3\rangle$. In particular, you should have found measurements for the third player that always give one of two post-measurement states:

$$\mathcal{M}_3^{b_3=0}(|\Psi_-^3\rangle) \rightarrow |\Psi_-^2\rangle, \quad \mathcal{M}_3^{b_3=1}(|\Psi_-^3\rangle) \rightarrow |\Psi_+^2\rangle,$$

where we define $\Psi_\pm^n = (|0\rangle^{\otimes n} \pm |1\rangle^{\otimes n})/\sqrt{2}$ and $\mathcal{M}_k^{b_k}$ denotes the (normalized) projector for a measurement on qubit k with outcome b_k.

a) Use the same measurement you found in 3.2 (*b*) (*ii*) to find the possible results of $\mathcal{M}_n(|\Psi_\pm^n\rangle)$: $M_n^0(|\Psi_+^n\rangle)$, $M_n^1(|\Psi_+^n\rangle)$, $M_n^0(|\Psi_-^n\rangle)$, and $M_n^1(|\Psi_-^n\rangle)$.

b) Explain a detailed quantum strategy that always wins this game.