Information Theory

Problem Set 1

0) Show that the Hamming distance on A^n satisfies the triangle inequality.

1) Consider the general binary channel pictured below. Suppose also that the input probability is given by $p = P(0)$ and $1 - p = P(1)$.

a) Call the channel with $\pi_1 = \pi_0 = \pi$ a *symmetric channel.* What is the relationship between the entropy of the input and that of the output?

b) Call the channel with $\pi_0 = 0$ a *half perfect channel.* Set $\pi_1 = \epsilon$. What is the relationship between the entropy of the input and that of the output?

2) In this problem we'll show that the general binary channel of problem 1) can be "factored" into simpler channels.

a) Suppose that $\pi_0 > \pi_1$, and that $\pi_0 > 1/2$. Find an ϵ and a π such that the half-perfect channel of 1b) followed by the perfect channel of 1a) gives the same output as the binary channel.

b) Show that the assumptions on π_0 in a) are not really needed. Any general binary channel can be factored as in a).

c) Can the general binary channel be factored in the opposite order, as a symmetric channel followed by a half-perfect channel?

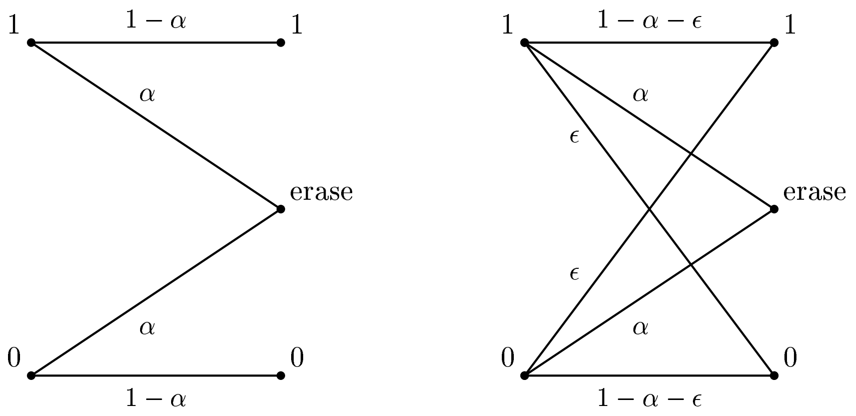
3) Consider the binary symmetric erasure and erasure/error channels illustrated in the diagrams.

a) Compute the capacity of the erasure channel. (Use the grouping law to simplify.)

b) Show that the capacity of the error/erasure channel is

$$(1 - \alpha)(1 - \log(1 - \alpha)) + (1 - \alpha - \epsilon)\log(1 - \alpha - \epsilon) + \epsilon \log \epsilon$$

(Argue that the input distribution achieving capacity is the uniform one, then simplify.)



(a) erasure channel (b) error/erasure channel

4) Suppose that we have a binary channel and that we use codewords of length $n = 7$. We wish to correct any occurrence of a single error. so the Hamming distance between any two codewords must be at least 3.

a) how many binary binary sequences (of length 7) have a distance of 1 or less from a given sequence?

b) What is the maximum number of codewords M that we can use if any single error is to be correctable?

c) Assuming the maximum can be achieved, what is the rate of the code?

5) Coin Weighing Problem: You are given n coins, exactly one of which is counterfeit. It is either heavier or lighter than the others, but you don't know which. Devise a strategy for discovering the counterfeit coin and it's relative weight using a balance.

a) Show it is possible using two weighings if $n = 3$.

b) Show it is possible using two weighings if $n = 4$ provided you have an extra coin that you know is good.

c) Show it is possible with 3 weighings if $n = 9$.

d) Consider now a different problem: You have n coins, one of which is counterfeit. k of the coins are known to not be heavier than a good coin and the rest are known to not be lighter than a good coin. Using a balance, how many weighings are needed to find the counterfeit coin and determine its weight? Solve this for small values of n.

e) Suppose now that you are given k coins which are not heavy, m coins which are not light, r coins which may be heavy or light, and you know that exactly one of the coins is counterfeit. Prove by induction that given an extra good coin, the counterfeit coin and its weight can be discovered in w weighings provided $3^w \geq k + m - 2r$.

f) Solve the original problem (n coins no extra good one).

Suggestion: A weighing determines a channel from the set of all possibilities for the counterfeit coin to the set of possible outcomes of the weighing. How much information is conveyed by the channel (with the uniform distribution on the choice of counterfeit coin)?