Homework 2
Due 2006/11/9

Oded Regev
Department of Computer Science
Tel Aviv University

Instructions

Collaboration: Collaboration is allowed, but limit yourselves to groups of size at most three.

References: Try not to run to reference material to answer questions (this also includes the web!). Try to think about the problem to see if you can solve it without consulting any external sources. If this fails, you may ask me for a hint, or look up any reference material.

Writeup: You must write the solutions by yourselves. For each question, cite all references used (or write 'none') and collaborators (or write 'alone'). Explain why you needed to consult any of the references.

Deadline: The deadline is strict.

Problems[1]

1. **Asymmetric binary channel:** Consider a channel whose input/output alphabet is $\{0, 1\}$, where a 0 is transmitted faithfully as a 0 (with probability 1), but a 1 is transmitted as 0 with probability $\frac{1}{2}$ and a 1 with probability $\frac{1}{2}$.

   (a) Compute the capacity of this channel. You should prove this from scratch using only simple probabilistic facts already stated/used in class. For partial credit, you may just prove a lower bound on the capacity. The higher your bound, the more the credit.

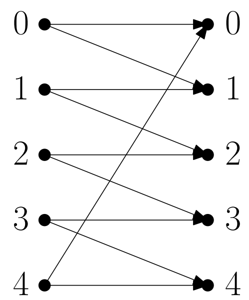
   (b) Verify your answer by computing the capacity of this channel according to the formula we mentioned in class. Namely, compute $\max I(X : Y)$ where Y is obtained from X using the channel, and the $\max$ goes over all distributions for X.

2. **Zero-error capacity:** Consider a channel with input/output alphabet $\{0, 1, \ldots, k-1\}$, where input symbol j is transmitted as j with probability $\frac{1}{2}$ and as $j + 1 \bmod k$ with probability $\frac{1}{2}$.

   (a) Compute the capacity of this channel using the formula we mentioned in class.

   (b) Define the *zero-error capacity* as the capacity of the channel achievable with an encoding whose error probability is zero. Clearly, this capacity is upper bounded by the usual channel capacity. Show that for even k, the zero-error capacity is equal to the channel capacity.

   (c) Consider the case $k = 5$. Clearly, the zero-error capacity in this case is at least 1 bit per symbol: we can transmit either 0 or 2 with probability $1/2$. Show that the zero-error capacity is strictly greater than 1 bit. Hint: consider codes of length 2



[1] Partly based on Madhu Sudan's problems

3. **Strengthening the lower bound on random access codes:** An (n, m, p) weak random access code consists of a randomized function f from $\{0,1\}^n$ to $\{0,1\}^m$ and randomized functions $g_1, \ldots, g_m$ where g_i is from $\{0,1\}^m \times \{0,1\}^{i-1}$ to $\{0,1\}$ such that

$$\forall i \in [n], \;\; \Pr[g_i(y, x_1, \ldots, x_{i-1}) = x_i] \geq p$$

where the probability is over a uniform choice of $x \sim \{0,1\}^n$ and a choice of $y \sim f(x)$. In words, g_i is supposed to guess x_i given the encoding $f(x)$ *and* the values $x_1, \ldots, x_{i-1}$.

   (a) Show that if Z is a randomized function of Y and W (i.e., $X \leftrightarrow YW \leftrightarrow Z$), then $I(Z : X|W) \leq I(Y : X|W)$ (this extends the data processing inequality).

   (b) Show that any (n, m, p) weak random access code must satisfy $m \geq (1 - H(p))n$.

   (c) What happens if we weaken the definition even further by also giving g_i access to $x_{i+1}, \ldots, x_n$?