Essential Coding Theory Madhu Sudan
6.896
Extended Due Date: Wednesday, October 2, 2002

Problem Set 2

Instructions: See PS 1.

Problems

1. Prove the noiseless coding theorem, and its converse. (But don't turn in.)

2. Consider a Markovian source of bits, where the source consists of a 6-cycle with three successive vertices outputing 0, and three successive vertices outputting 1, with the probability of either going left (or right) from any vertex is exactly 1/2. Compute the rate of this source. (I expect an ab initio argument. Hopefully this will motivate you to look up Shannon's general method for computing the rate of a Markovian source.)

3. Consider a binary 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 a 0 with probability $\frac{1}{2}$ and a 1 with probability 1/2. Compute the capacity of this channel. (You should prove this from scratch using only simple probabilistic facts already stated/used in class - not by referring to tools gleaned from other courses in information theory. For partial credit, you may just prove a lower bound on the capacity. The higher your bound, the more the credit.)

4. If there is a constructive solution to Shannon's noisy coding theorem with E being a linear map, then show that there is a constructive solution to Shannon's noiseless coding theorem in the case where the source produces a sequence of independent bits of bias p.

   Clarifications:

   (a) The encoding and decoding functions used in the noiseless theorem should be polynomial time computable, if the corresponding functions are polynomial time computable in the noisy theorem.

   (b) The compression rate in the noiseless coding theorem should be arbitrarily close to $H(p)$, assuming the rate of the encoding function in the coding theorem can be made arbitrarily close to $1 - H(p)$.

5. Given codes C_1 and C_2 with encoding functions $E_1 : \{0, 1\}^{k_1} \to \{0, 1\}^{n_1}$ and $E_2 : \{0, 1\}^{k_2} \to \{0, 1\}^{n_2}$ let $E_1 \otimes E_2 : \{0, 1\}^{k_1 \times k_2} \to \{0, 1\}^{n_1 \times n_2}$ be the encoding function obtained as follows: View a message $\mathbf{m}$ as a $k_1 \times k_2$ matrix. Encode the columns of $\mathbf{m}$ individually using the function E_1 to get an $n_1 \times k_2$ matrix $\mathbf{m}'$. Now encode the rows of $\mathbf{m}'$ individually using E_2 to get an $n_1 \times n_2$ matrix that is the final encoding under $E_1 \otimes E_2$ of $\mathbf{m}$. Let $C_1 \otimes C_2$ be the code associated with $E_1 \otimes E_2$.

   For $i \geq 3$, let H_i denote the $[2^i - 1, 2^i - i - 1, 3]_2$-Hamming code. Let $C_i = H_i \otimes C_{i-1}$ with $C_3 = H_3$ be a new family of codes.

(a) Give a lower bound on the relative minimum distance of C_i. Does it go to zero as $i \to \infty$?

(b) Give a lower bound on the rate of C_i. Does it go to zero as $i \to \infty$?

(c) Consider the following simple decoding algorithm for C_i: Decode the rows of the rec'd vector recursively using the decoding algorithm for C_{i-1}. Then decode each column according to the Hamming decoding algorithm. Let p_i denote the probability of decoding error of this algorithm on the Binary Symmmetric Channel with parameter p. Show that there exists a $p > 0$ such that $p_i \to 0$ as $i \to \infty$. (Hint: First show that $p_i \leq 4^i p_{i-1}^2$.)