Essential Coding Theory
6.440
Due: Friday, March 7, 2008

Lecturer: Madhu Sudan
TA: Swastik Kopparty

Problem Set 2

Instructions

References: In general, try not to run to reference material to answer questions. Try to think about the problem to see if you can solve it without consulting any external sources. If this fails, you may look up any reference material.

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

Writeup: You must write the solutions by yourselves. Cite all references and collaborators. Explain why you needed to consult any of the references, if you did consult any. Submit the solutions electronically as a pdf file. Deadline is 11pm on due date.

Problems

1. (Shannon Capacity of an asymmetric channel): Let $p \in [0,1]$. Consider a channel $C : \{0,1\} \to \{0,1\}$ that operates as follows:

   - On input 0, it always outputs 0.
   - On input 1, it outputs 0 with probability p and and 1 with probability $1-p$.

   The channel acts independently each time it is used. Determine the Shannon Capacity of this channel C.

   Please try to build a proof "from scratch", i.e., not using 6.441 material. Specifically, show that a random encoding function from some appropriate distribution achieves a rate arbitrarily close to your claimed capacity. Show also that every encoding/decoding function with rate better than your claimed capacity errs with all but exponentially small probability.

2. (Random codes and the Gilbert-Varshamov bound): Here we will study the distance of a random code, and how to modify it so that meets the Gilbert-Varshamov bound.

   (a) Let $R \in [0,1]$ and let $k = Rn$. Pick "codewords" $c_1, c_2, \ldots, c_{2^k}$ independently and uniformly at random from $\{0,1\}^n$, and set $C = \{c_i : i \in [2^k]\}$. Show that for any δ satisfying $H(\delta) > 1 - 2R$, with probability $\to 1$ as $n \to \infty$, the distance of the code C at most δn. Thus for $R > 0$, such a randomly chosen code *does not* meet the Gilbert-Varshamov bound.

   (b) Let R and C be as in the previous part and now let $\delta' \in [0,1]$ satisfy $H(\delta') > 1 - R$. Let $C' = \{c_i \in C \mid \forall j \in [i-1], d_H(c_i, c_j) \geq \delta' n\}$. Clearly the distance of C' is at least $\delta' n$.

Show that for sufficiently large n, with probability $\geq 1/3$, $|C'| \geq \frac{2^k}{3}$. Thus C' meets the Gilbert-Varshamov bound.

3. (q-ary Plotkin bound): Let $q \geq 2$ be an integer and let $R, \delta \in [0,1]$. Prove that for any family of codes $C_n \subseteq [q]^n$, with rate $\to R$ and relative distance $\to \delta$,

$$R + \frac{q}{q-1}\delta \leq 1.$$

4. Explicitness of the Justesen codes: Recall that for integer $t > 0$ and $0 < k < 2^t$, the Justesen code $J_{t,k}$ maps kt bits to $2nt$ bits where $n = 2^t - 1$. Give a polynomial time algorithm that takes as input the tuple (t, k, i, j) where $1 \leq i \leq kt$ and $1 \leq j \leq 2nt$ and computes the (i, j)th entry of the generator matrix of $J_{t,k}$.