CSC 2414H - Assignment 1

Due Jan 31 , 2008

General rules : In solving this you may consult books and you may also consult with each other, but you must each write your own solution. In each problem list the people you consulted. This list will not affect your grade.

1. Recall that in order to prove the first part of Shannon's theorem, we have seen the following: If we take a random encoding function from k to n bits such that $R = k/n < 1 - H(p)$, then for every $m \in \{0,1\}^k$

$$\Pr_{\mathrm{E},\eta\in\mathrm{BSC(p)}}[\mathrm{D(E(m)}+\eta)\neq \mathrm{m}] \leq 2^{-\Omega(\mathrm{n})}.$$

   Using this it was easy to show that there is an encoding function such that

$$\Pr_{\mathrm{m}\in\{0,1\}^{\mathrm{k}},\eta\in\mathrm{BSC(p)}}[\mathrm{D(E(m)}+\eta)\neq \mathrm{m}] \leq 2^{-\Omega(\mathrm{n})}.$$

   Extend this result to show the existence of encoding and decoding functions E, D, such that *for all* $m \in \{0,1\}^k$

$$\Pr_{\eta\in\mathrm{BSC(p)}}[\mathrm{D(E(m)}+\eta)\neq \mathrm{m}] \leq 2^{-\Omega(\mathrm{n})}$$

   Hint: Consider using a random code as before, but use only the best (in some sense) half of the codewords, discarding the rest. Show that the code you get has the desired property and that the rate, although smaller, is asymptotically the same as in the original analysis.

2. We use the following notation. An $(n,k,d)_q$ code is a code with q^d code words of length n with alphabet $\mathbb{F}_q$, and with distance d. An $[n,k,d]_q$ is defined similarly except the code is linear. If one of the parameters does not appear we simply ignore it.

   (a) Let L be a binary $[n,k]_2$ code and suppose that it contains a word with odd weight (the weight of a word is the number of nonzero characters). Prove that the words of even weight in L form a binary $[n,k-1]_2$ code.

   (b) If an $(n,k,d)_2$ with d odd exists then an $(n+1,k,d+1)_2$ code also exists.

   (c) Show that the condition on d being odd in (b) is necessary by giving an example of an $(n,k,d)_2$ code (for some values of n,k,d of your choice) such that no $(n+1,k,d+1)_2$ code exists.

(d) Show part (b) for linear codes.

3. (Shannon's theorem for deletions) Consider the binary deletion channel: Here, bits are deleted instead of being flipped. So the deletion channel with error probability p will transmit a bit correctly with probability $1-p$ and will delete its content with probability p independently. For example 0011001 may be received as 0??1001 (notice that the receiver is aware of every deletion and its bit position). We use the notation $\eta \in \mathrm{BDC(p)}$ to mean that η is a random string of deletions with parameter p. Your goal is to show a similar statement to that of Shannon's theorem. Explicitly:

   (a) if $R < 1-p$ then there is an encoding and decoding functions so that

   $$\Pr_{\mathrm{m}\in\{0,1\}^{\mathrm{k}},\eta\in\mathrm{BDC(p)}}[\mathrm{D(E(m) \text{ with deletions according to } } \eta) \neq \mathrm{m}] \leq 2^{-\Omega(\mathrm{n})}.$$

   (b) If $R > 1-p$ then for all E, D

   $$\Pr_{\mathrm{m}\in\{0,1\}^{\mathrm{k}},\eta\in\mathrm{BDC(p)}}[\mathrm{D(E(m) \text{ with deletions according to } } \eta) = \mathrm{m}] \leq 2^{-\Omega(\mathrm{n})}.$$

   In addition

   (c) We call the critical values $1-H(p)$ for the binary symmetric channel, and $1-p$ for the binary deletion channel, the *capacity* of the channel. Which of the two capacities is bigger? Can you give a simple explanation?

4. Consider transmitting a message $m \in \{0,1\}^k$ in the Binary Symmetric Channel (BSC(p)) using the simple "duplication code". That is, the encoding function copies the message r times, where r is some positive integer, so $n = kr$.

   (a) Show that the duplication code is a linear code, and give its generator matrix G and its parity check matrix H. What is the distance of the code?

   (b) Give a lower bound to the probability that a random message fails to be decoded correctly. Compare to Shannon's theorem and conclude that the duplication code has poor performance.