Homework 5: Due Apr 19th on Dropbox in Angel

Posted on April 7th

Collaboration policy: You are allowed to discuss homework problems with your classmates. However, you should think about the problems before discussing them, and you must write up your own solutions. You must acknowledge any collaboration by writing your collaborators names on the front page of the assignment.

Citation policy: Try to solve the problems without reading any published literature or websites, besides the textbook and notes from class. If, however, you do use a solution or part of a solution that you found in the literature or on the web, you must cite it. Furthermore, you must write up the solution in your own words.

Submission: Homeworks typeset in latex are encouraged. If you submit a hand-written homework, please ensure that it is written legibly. The homeworks must be uploaded in the dropbox provided on Angel.

Grading: Every question is worth 10 points.

1. Consider the convolutional code

$$v^{(1)}(j) = u(j) + u(j-1)$$
$$v^{(2)}(j) = u(j) + u(j-1) + u(j-2)$$

   (a) Write the state diagram and trellis diagram (for one stage) of the code.

   (b) Write the output bits assuming that the input bits are 0110.

   (c) Assume that the receiver receives 11 00 01 11 00. Determine the most likely input bit string. (If there is a tie, pick one of them.)

   (d) Express the code in systematic form, and write its trellis diagram (for one stage).

2. Prove that the conventional Reed Solomon code, where the evaluation points are n roots of unity, is cyclic. That is, prove that if $(c_0, c_1, \ldots, c_n)$ is a codeword, then prove that both $(c_1, c_2, \ldots, c_n, c_0)$ and $(c_n, c_0, c_1, \ldots, c_{n-1})$ are also codewords.

3. In this question, you will explore some ingredients that prove the capacity of the binary symmetric channel. Recall from Homework 1, that the probability that a random n-length sequence $\vec{y}$ lies in the Hamming ball $B(\vec{0}, np)$ is equal to $2^{-n(1-H(p))+o(n)}$. Now, we will construct a codebook as

$$\mathcal{C} = \{\vec{0}, \vec{x}_1, \vec{x}_2, \ldots, \vec{x}_{2^k-1}\}$$

   where $\vec{x}_1, \ldots, \vec{x}_{2^k-1}$ are randomly and independently chosen. The entries of these vectors are chosen in i.i.d manner with $\Pr(x_{i,j} = 0) = \Pr(x_{i,j} = 1) = 1/2$, where $x_{i,j}$ is the jth component of $\vec{x}_i$.

   The codebook is used over the binary symmetric channel with probability p. To show capacity, we will show that if $k/n \leq 1 - H(p) - \epsilon$, then for any $\epsilon > 0$, the probability of error goes to 0 as $n \to \infty$. Rather than show it for every codeword, to keep things simple, we will show this for the all zeroes codeword.

   (a) Assume that the all zeroes codeword is transmitted over the BSC, and the received vector is $\vec{y}$. Prove that $\vec{y} \in B(\vec{0}, np + n\epsilon/2)$ with a probability that tends to 1 as $n \to \infty$. *Hint: Use the weak law of large numbers on the total number of bit flips caused by the channel.*

(b) Use the above result to show that $\vec{0} \in B(\vec{y}, np + n\epsilon/2)$, with probability that tends to 1 as $n \to \infty$.

(c) Use the result of Homework 1 and the fact that $\vec{x}_i$ is independent of the transmitted codeword, and hence the vector $\vec{y}$, to show that $\Pr(\vec{x}_i \in B(\vec{y}, np + n\epsilon/2)) \leq 2^{-n(1-H(p))+n\epsilon/2+o(n)}$. *Hint: the only difference from Homework 1 is that the ball is centered around $\vec{y}$ and not $\vec{0}$. Does this make a difference?*

(d) Note the following equations.

$$\begin{aligned}
\Pr(\text{Error}|\vec{0} \text{ transmitted}) &= \Pr\left(\bigcup_{i=1}^{2^k-1} d_H(\vec{y}, \vec{x}_i) \leq d_H(\vec{y}, \vec{0})\right) \\
&\overset{(a)}{\leq} \Pr\left(\bigcup_{i=1}^{2^k-1} \vec{x}_i \in B(\vec{y}, np + n\epsilon/2)\right) \\
&\overset{(b)}{\leq} \sum_{i=1}^{2^k-1} \Pr\left(\vec{x}_i \in B(\vec{y}, np + n\epsilon/2)\right) \\
&\overset{(c)}{\leq} 2^{k-n(1-H(p))+n\epsilon/2+o(n)}
\end{aligned}$$

Give reasons for (a), (b), and (c) above and describe your conclusion regarding the the probability of error as $n \to \infty$ if $k \leq n(1 - H(p) - \epsilon)$.