

Date Assigned: 13 October 2004.

Date Due: 20 October 2004 in class.

Suggested Reading: Chapter 8 of your text book: Sections 8.5 through 8.12. We didn't cover Section 8.11 on Hamming codes and instead covered codes for the BEC; the reading material for this part will be provided in one of the exercises below.

1. Exercises 8.7 through 8.12 of the text book.
2. Theorem 8.2.1 (page 190 of your book) states that the optimal input distribution is uniform for weakly symmetric channels. How about the converse? Find a channel that is not weakly symmetric but the optimal input distribution is still uniform or show that there are none.
3. *Linear Codes for the Binary Erasure Channel:* Linear codes with rate $R = k/n$ are parameterized by a $k \times n$ matrix \mathbf{A} : the sequence of k information bits results in n bits transmitted over the channel. The n coded bits are simply the information bits operated linearly upon by \mathbf{A} . Fix $\epsilon > 0$ and $k = (1 - p - \epsilon)n$. So, the rate of the code is $1 - p$. Consider using this code over the BEC with erasure probability p .
 - (a) Show that the probability that more than a fraction $(1 - p + \epsilon)$ of the n transmitted bits are erased goes to zero as n grows large.
 - (b) Conclude that we can correctly decode *any* information bit sequence with high probability provided every $k \times (1 - p + \epsilon)n$ sub-matrix of A has full rank.
 - (c) Now we consider construction of linear codes that have the above mentioned property. This part is a reading exercise; you don't need to turn in anything.
 - i. **Random Linear Codes:** Consider the random linear code: each entry of \mathbf{A} is i.i.d. 0 or 1 with probability 0.5 each. A reading exercise is to study <http://www.ece.umd.edu/~abarg/ENEE739C/lecture7.pdf>, where it is shown that almost surely the random linear matrix \mathbf{A} has the desired rank property. Thus it is easy to construct linear codes that work for the BEC (almost every random linear code works). The problem is that the decoding complexity – which involves inverting a $(1 - p)n \times (1 - p)n$ matrix – is $O(n^3)$.
 - ii. **Reed-Solomon Codes:** These are *structured* linear codes that guarantee the decodability condition. They also have the additional property that their decoding complexity is smaller: $O(n^2)$. Reed-Solomon codes are used in several data storage applications: for example, hard disks and CDs. You can learn about these codes from *any* text book on coding theory.

iii. **Digital Fountain Codes:** These are a new class of random linear codes that satisfy the decodability condition with very high probability. The distinguishing feature is that the matrix \mathbf{A} is very sparse, i.e., most of its entries are 0. The key feature is a simple decoding algorithm that has complexity $O(n \log(n/\delta))$ with probability larger than $1 - \delta$. For a wide class of channels, a sparse linear code admits a simple decoding algorithm, called the *message passing algorithm*. It is very fundamental and has been rediscovered over the decades by very diverse areas of applied mathematics and engineering: the Kalman filter, the belief propagation algorithm, the fast Fourier transform are all instances. This is a very recent development that has revolutionized coding theory, both theoretically and from a practical point of view. Here are a few references for you to learn more about this exciting area.

- There is an entire book on the subject of message passing algorithms as viewed in coding theory. It is titled *Modern Coding Theory* and a draft is available at lthcwww.epfl.ch/papers/ics.ps .
- A good introduction to Fountain codes is available at <http://www.inference.phy.cam.ac.uk/mackay/DFountain.html> .
- Some students might be interested in checking out <http://www.digitalfountain.com> .