EECS 121 Coding for Digital Communication and Beyond

Fall 2013 Anant Sahai MT 1

PRINT your student ID: ____________________________________

PRINT AND SIGN your name:

________________, ________________ ____________________

(last) (first) (signature)

PRINT your Unix account login: ee121-____________

Prob. 1	
Prob. 2	
Prob. 3	
Total	

You may consult your one handwritten note sheet. **(You must turn it in with your exam.)** Phones, calculators, tablets, and computers are not permitted. No collaboration is allowed at all and you are not allowed to look at another's work.

Please write your answers in the spaces provided in the test; in particular, we will not grade anything on another exam page unless we are clearly told in the problem space to look there.

You have 80 minutes. There are 3 questions, of varying numbers of points. The questions and their parts are of varying difficulty, so avoid spending too long on any one part.

50 Points is a good score. This is basically a two hour exam but you only have one hour and twenty minutes.

Do not turn this page until your instructor tells you to do so.

Problem 1. [True or false] (10 points)

Circle TRUE or FALSE.

Prove statements that you think are true and disprove (e.g. by showing a counterexample) statements that you think are false.

(a) TRUE or FALSE: Consider an iid sequence of Bernoulli-p random variables X_i for $p < \frac{1}{2}$. Suppose that we define the Typical Set $T_\varepsilon^n = \{\vec{x} \in \{0,1\}^n | 2^{-n(H(p)+\varepsilon)} \leq P(\vec{X} = \vec{x}) \leq 2^{-n(H(p)-\varepsilon)}\}$ for $\varepsilon > 0$. Here $H(p) = p \log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}$.

Then the set T_ε^n contains the most likely binary sequence — *i.e.* the n-length sequence $\vec{x}$ that maximizes $P(\vec{X} = \vec{x})$.

Problem 2. Not quite orthogonal signaling (40 points)

Consider a continuous-time channel over the time-interval $[0,1]$ with AWGN $N(t)$ with intensity 1. (e.g. $\int_0^1 N(t)dt$ is a standard Gaussian random variable with mean 0 and variance 1.)

The signaling being used is a kind of pulse-position modulation where the potential pulses sometimes overlap with each other. There are 2^k possible pulses for messages corresponding to $i = 0, 1, \ldots, 2^k - 1$.

$$x_i(t) = \begin{cases} 0 & \text{if} \quad t < \frac{i}{2^k+1} \\ \sqrt{P\frac{2^k+1}{2}} & \text{if} \quad \frac{i}{2^k+1} \le t \le \frac{i+2}{2^k+1} \\ 0 & \text{if} \quad t > \frac{i+2}{2^k+1} \end{cases}$$

The decoding strategy will be the same general correllate and then threshold strategy. So $\widetilde{Y}_i = \int_0^1 Y(t)\frac{x_i(t)}{\sqrt{P}}dt$ will be calculated and then compared against a threshold T to see which one passes.

a. (4 points) Sketch what these waveforms look like for some generic i, $i+1$, and $i+2$.

b. (5 points) Show that $\|x_i\|^2 = P$.

c. (6 points) Calculate $\langle x_i, x_j \rangle$. Are they all orthogonal to each other?

d. (20 points) Choose a (good) formula for a threshold T and argue why the probability of the true $\widetilde{Y}_m > T$ should approach 1 as k increases while the probability that all false $\widetilde{Y}_f < T$ should approach 1 as k increases.

(HINT: Now there are two kinds of false codewords — those that are not orthogonal to the true codeword and those that are. Deal with them separately.)

(Second HINT: Feel free to guess at the threshold and move on to the next part. Come back to finish this later.)

[Extra Page]

e. (5 points) What is the energy per bit required in your scheme from part (c) for successful decoding? Comment.

PRINT your name and student ID: ____

Problem 3. Random Affine Codes with a twist (35 points)

In this problem, you are asked to consider a different approach to coming up with random affine codes.

We are going to be working in a finite field F_n of size 2^n. This means that there is an addition, additive inverses, multiplication, and multiplicative inverses, etc. For this problem, feel free to assume that all the properties you learned in 70 about finite fields of prime sizes continue to apply to this field F_n so you can also invoke polynomial properties including properties of roots, degrees, interpolation, etc. as you would like.

Furthermore, assume there is an **invertible** mapping $g(\vec{x})$ that maps a n-bit binary string $\vec{x}$ into an element of this field and g^{-1} does the reverse.

The messages $\vec{d}$ are k-bits long and can be interpreted as n-bit binary strings by simply putting zeros in front. So assume that you can apply g to messages $\vec{d}$ as well.

(HINT: It might help to just ignore g throughout the problem and just believe that multiplication of these vectors is a magical operation that obeys finite field rules.)

Consider a randomized coding strategy that works as follows:

1. Two elements of the finite field F_n are drawn iid uniformly at random. Call these A and B. This is done at design time so that both the encoder and decoder know A and B.
2. n-bit codewords are generated for k-bit messages $\vec{d}$ using $\vec{x}(\vec{d}) = g^{-1}(A * g(\vec{d}) + B)$ where the $*$ represents multiplication in F_n and the $+$ represents addition in F_n.

a. (5 points) Show that the codeword corresponding to a message $\vec{d}$ is drawn uniformly at random from all 2^n possible codewords.

b. (10 points) Show that the codewords corresponding to different mesages are pairwise independent.

(HINT: Feel free to skip this part and come back to it later. You won't need this part for the next parts.)

c. (5 points) From parts (a) and (b), you can see that all the properties we required in the in-class random-coding analysis are satisfied and these random codes will work as well as those discussed in lecture. **How many bits does it take to represent a particular code?** (*i.e.* specify the A and B)

d. (5 points) Further suppose that the mapping g has the following properties: $g(\vec{0}) = 0$, $g(\vec{v}+\vec{w}) = g(\vec{v}) + g(\vec{w})$ for all $\vec{v}$ and $\vec{w}$. (*i.e.* It's as though the addition operation in F_n operates bitwise.)

Argue why in this case, for use over a binary symmetric channel, it suffices to just use linear codes $g^{-1}(A * g(\vec{d}))$**.** (A binary symmetric channel is the channel discussed in class that looks like additive iid Bernoulli-p noise in the binary field.)

e. (10 points) Keeping the assumptions of part (d) above, are the resulting codes linear codes when viewed over binary vectors? (*i.e.* For every A does there exist a matrix G so that $g^{-1}(A * g(\vec{d})) = G\vec{d}$ for all $\vec{d}$?)

(HINT: Can you interpret the columns of G? Then check that interpretation…)

[Extra Page]