3 problems, 110 points
3 hours
2 sheets of notes allowed

Good Luck!

PLEASE WRITE YOUR NAME ON EACH SHEET OF YOUR ANSWERS

PLEASE USE A SEPARATE SHEET FOR ANSWERING EACH QUESTION

PROBLEM 1. (30 points)

(a) (5 pts) [A useful lemma.] Suppose $E_1, \dots, E_M$ are independent events, each with probability $1-p$. Show that $\Pr(\cap_i E_i) \le \exp(-pM)$. [*Hint:* $\ln(1-p) \le -p$.]

We will analyze a random code construction for *source coding.*

A source produces i.i.d. letters from an alphabet $\mathcal{U}$ according to a distribution $p_U$. A block source coding scheme is constructed as follows:

1. Pick a blocklength $n$ and rate $R$.

2. Randomly pick $M = 2^{nR}$ sequences of length $n$,

$$\mathbf{U}(1), \dots, \mathbf{U}(M),$$

   choosing each letter of each sequence independently according to the distribution $p_U$. Reveal these choices to the encoder and decoder.

3. The encoder operates as follows: When asked to encode a sequence $\mathbf{u} \in \mathcal{U}^n$, the encoder searches for an $m = 1, \dots, 2^{nR}$ for which $\mathbf{u} = \mathbf{U}(m)$. If such an $m$ is found, the encoder outputs $m$ (as an $nR$ bit integer). If no such $m$ is found the encoder uses $m = 1$.

4. The decoder, when asked to decode an $nR$ bit integer $m$, outputs $\mathbf{U}(m)$.

We will now analyze the probability that this randomly constructed encoder/decoder pair makes an error, i.e., $\Pr\{\mathrm{Dec}(\mathrm{Enc}(\mathbf{U})) \neq \mathbf{U}\}$.

(b) (5 pts) Suppose the sequence to be encoded is $\mathbf{u}$. Show that

$$\Pr\{\mathrm{Dec}(\mathrm{Enc}(\mathbf{u})) \neq \mathbf{u}\} \le \exp(-p_{U^n}(\mathbf{u})M).$$

(c) (10 pts) Suppose that the sequence $\mathbf{u} = (u_1, \dots, u_n)$ is $\epsilon$-typical (in the sense that $\frac{1}{n}\#\{i : u_i = a\} = (1 \pm \epsilon)p_U(a)$ for each $a \in \mathcal{U}$). Show that

$$\Pr(\mathrm{Dec}(\mathrm{Enc}(\mathbf{u}) \neq \mathbf{u})) \le \exp(-2^{n[R-(1+\epsilon)H(U)]}).$$

(d) (10 pts) Show that if $R > H(U)$ the encoding method described above will have an error probability that approaches zero as $n$ gets large.

PROBLEM 2. (40 points)

(a) (5 pts) Suppose $f(\beta)$ is a concave-$\cap$ function defined on $[0,\infty)$ with $f(0)=0$. Show that $f(\beta)/\beta$ is a decreasing function on $(0,\infty)$.

[*Hint:* if $0<\beta_1<\beta_2$, then $\beta_1=(1-\lambda)0+\lambda\beta_2$ with $\lambda\in[0,1]$.]

Suppose we have a discrete memoryless channel with a binary input alphabet $\mathcal{X}=\{0,1\}$. Let $p(y|x)$ denote the channel transition probabilities. The inputs to the channel carry a cost, the cost of the symbol $x$ is $x$ (i.e., the symbol 0 is free, the symbol 1 has a unit cost).

(b) (10 pts) Let $I(\beta)$ denote the mutual information between the input and output of the channel when $\Pr(X=1)=\beta$, and $C(\beta)$ the capacity under cost constraint $\beta$. Express $C(\beta)$ in terms of $I(\beta)$.

(c) (10 pts) The quantity $\sup_{\beta>0} C(\beta)/\beta$ is the largest number of bits per cost we can reliably transmit across a channel and is called the *capacity per cost*. Show that

$$\sup_{\beta>0}\frac{C(\beta)}{\beta}=\lim_{\beta\searrow 0}\frac{I(\beta)}{\beta}.$$

[*Hint:* use what you showed in part (a)]

(d) (10 pts) Show that $\lim_{\beta\searrow 0}\frac{I(\beta)}{\beta}=\sum_y p(y|1)\log\frac{p(y|1)}{p(y|0)}$.

(e) (5 pts) What is the capacity per cost of the binary symmetric channel with cross-over probability $p$?

PROBLEM 3. (40 points) Consider a linear code defined over the ternary alphabet $\mathbb{F}_3 = \{0, 1, 2\}$ (equipped with modulo-3 addition and multiplication) as follows: $\mathbf{x}$ is a codeword if and only if $H\mathbf{x} = \mathbf{0}$ where

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

(and all operations are done in modulo-3 arithmetic).

(a) (5 pts) What is the blocklength, the number of codewords, and the rate of this code?

A codeword $\mathbf{x}$ is sent over a channel. It is known that during the transmission either all letters are received correctly, or, one of the letters is changed (to some other element of $\mathbb{F}_3$).

(b) (10 pts) Show that the receiver can detect if a change has happened and correct it if so.

(c) (5 pts) Suppose we are allowed to augment the matrix $H$ by appending to it a fifth column. How will this change the rate of the code?

(d) (10 pts) Which of the following candidate columns (if any) can be appended to $H$ and still preserve the property in (b): $\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 \\ 2 \end{smallmatrix}\right]$?

(e) (10 pts) Suppose it is known that during the transmission all letters are received correctly, or one of the letters is changed in the following restricted way: 0 can be replaced by 1 (but not by 2); 1 can be replaced by 2 (not by 0); 2 can be replaced by 0 (not by 1). Redo part (d) for this channel.