ECE 520.447
Introduction to Information Theory and Coding

Midterm Examination #2

9:00 — 9:50 AM, November 25, 2002.

Name: ____

Read these instructions before starting the examination.

(i) This is a open-book examination. Use of any one textbook is permitted. Photocopied material from other books, handwritten/class notes, *etc.* are not permitted.

(ii) Use of electronic calculators is permitted for numeric calculations only.

(iii) Show all your work clearly and concisely. Points may be deducted for illegible or unclear answers.

(iv) Provide answers in the space provided. Use the unprinted side of the pages in the examination booklet if necessary.

(v) There are three mandatory questions for a total of 50 points.

Best of luck!

Question № 1	/10 Points
Question № 2	/20 Points
Question № 3	/20 Points
TOTAL	/50 Points

Question No 1: *The two-look Gaussian channel.* Consider the usual discrete time memoryless Gaussian channel without feedback, with the modification that the transmitted symbol X is received at two distinct receivers as Y_1 and Y_2, and the decoder has access to both Y_1 and Y_2. This, for example, is the situation in an antenna-array. The noise in the two observations is, in general, going to be correlated. Assume that

$$\begin{aligned} Y_1 &= X + Z_1, \\ Y_2 &= X + Z_2, \end{aligned}$$

the transmitter has a signal power constraint P, and the noise vector $Z = [Z_1 \ Z_2]^{\mathrm{T}}$ is independent of X and is jointly Gaussian with zero mean and covariance matrix

$$K_Z = \begin{bmatrix} N & \rho N \\ \rho N & N \end{bmatrix}$$

1(a) Compute the capacity of this channel in terms of P, N and ρ. (5 points)

1(b) What is the capacity when $\rho = 1$? Interpret your answer by comparing it with the capacity of a *one observation* Gaussian channel with power constraint P. (1 points)

1(c) What is the capacity when $\rho = 0$? Interpret your answer by comparing it with the capacity of a *one observation* Gaussian channel with power constraint P. (2 points)

1(d) What is the capacity when $\rho = -1$? Provide an intuitive explanation for the answer by describing a simple decoding scheme which achieves capacity. (2 points)

Question No 2: Let $\mathcal{X} = \mathcal{X}_1 \bigcup \mathcal{X}_2 \bigcup \mathcal{X}_3$ and $\mathcal{Y} = \mathcal{Y}_1 \bigcup \mathcal{Y}_2 \bigcup \mathcal{Y}_3$ represent the input and output alphabet respectively of a discrete memoryless *sum channel* with three subchannels — i.e. a channel in which there is no cross-over from input symbols in $\mathcal{X}_i$ to output symbols in $\mathcal{Y}_j$ for $i \neq j$. Stated differently, the channel transition probabilities can be arranged as a block diagonal matrix:

$$[p(y|x)] = [w_{xy}] = W = \begin{bmatrix} W_1 & 0 & 0 \\ 0 & W_2 & 0 \\ 0 & 0 & W_3 \end{bmatrix} \qquad (1)$$

2(a) Draw the channel transition diagram for the specific case of

$$\mathcal{X}_1 = \{1, 2\} = \mathcal{Y}_1, \qquad \mathcal{X}_2 = \{3, 4\} = \mathcal{Y}_2, \qquad \mathcal{X}_3 = \{5, 6\} = \mathcal{Y}_3,$$

where each subchannel W_1, W_2 and W_3 is a binary symmetric channel with cross-over probability $\frac{1}{2}$. Write the 6×6 transition matrix W for this channel. (4 points)

2(b) What is the capacity of the channel described in 2(a) above? (4 points)

2(c) Show that the capacity C of the general sum channel W of equation (1), *not* the specific case of 2(a), is given by

$$2^C = 2^{C_1} + 2^{C_2} + 2^{C_3},$$

where C_1, C_2, and C_3 are the capacities of the individual channels W_1, W_2 and W_3 respectively.[*Hint*: Define a random variable

$$Z = \begin{cases} 1 & \text{if } X \in \mathcal{X}_1, \\ 2 & \text{if } X \in \mathcal{X}_2, \\ 3 & \text{if } X \in \mathcal{X}_3, \end{cases}$$

and exploit the equalities $H(Y) = H(Y, Z)$ and $H(Y|X) = H(Y|X, Z)$ (why?) to express $I(X;Y)$ in terms of $I(X;Y|Z)$ and $H(Z)$.] (8 points)

2(d) Compute the capacity of a channel with input alphabet $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7, 8\}$, output alphabet $\mathcal{Y} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and channel transition probabilities $p(y|x)$

given by

$$[p(y|x)] = [w_{xy}] = \begin{bmatrix} \frac{2}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & \frac{1}{3} & 0 & 0 & 0 & \frac{1}{3} & 0 & \frac{1}{3} & 0 \\ \frac{1}{3} & 0 & 0 & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & \frac{2}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 \end{bmatrix}.$$

[*Hint*: Draw the channel transition diagram.] (4 points)

Extra Work Space

Question No 3: This problem develops another lower bound, similar to the *Hamming* bound of your homework assignment, on the error correcting capability of a (n, k) *binary* linear block code in terms of n and k. The bound developed here is called the *Plotkin* bound.

3(a) Show that minimum Hamming distance d_{min} between two codewords of a binary linear block code is equal to the Hamming weight of the codeword with the smallest number of 1's, excluding the all-0 codeword. (4 points)

Consider an (n, k) binary linear block code whose generator matrix $\mathbf{G}$ does not contain any all-zero row. An example of such a matrix is

$$\mathbf{G} = \begin{bmatrix} I_{4\times 4} \\ P_{3\times 4} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}, \tag{2}$$

the generator of the $(7, 4)$ Hamming code we studied in class. A k-bit message vector $\mathbf{m}$ generates a n-bit codeword vector $\mathbf{c} = \mathbf{G} \times \mathbf{m}$. *e.g.* For

$$\mathbf{m} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \qquad \mathbf{c} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Let $\mathbf{C}$ be the $n \times 2^k$ matrix in which each column is an n-bit codeword for one of the 2^k distinct k-bit messages. For the generator matrix of equation (2), for example,

$$\mathbf{C} = \mathbf{G} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

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

3(b) Show that for any (n, k) binary linear block code (i.e. not just the particular (7,4) code shown above), each row of $\mathbf{C}$ contains exactly 2^{k-1} 0's and 2^{k-1} 1's. [*Hint*: What is the relationship between the (i, j)-th component of $\mathbf{C}$ and the i-th row of $\mathbf{G}$? What happens as j goes from 0 to 2^k?] (8 points)

3(c) Show that the minimum distance $d_{\min}$ of an (n, k) binary linear block code satisfies

$$d_{\min} \le \frac{n \cdot 2^{k-1}}{2^k - 1}. \tag{3}$$

[*Hint*: The result of 3(b) states how many 1's there are in the ensemble **C** of all the codewords. The result of 3(a) states how $d_{\min}$ relates to the number of 1's in one particular codeword.] (8 points)

Extra Work Space