

ECE1502S — Information Theory Midterm Test

Instructions

- You have one hour and fifty minutes of “in-class” time, followed by two days of “take-home” time to complete this test.
- Complete as much as possible during the in-class time; your grade will be computed as a weighted average of your “in-class” grade and your “take-home” grade. (Weights to be determined later.)
- Answer **all** questions. The value of each question is indicated beside the question. Show all steps and present all results clearly.
- Take-home due date: Thursday, March 2, 2006, 1:00 pm (in class). Please return a *complete* solution for the take home portion, even if you believe that you answered the question correctly in class.
- All aids are permitted during the take-home portion, but **all work is to be done independently**. (No mutual information!) Consultation with others is **not** permitted.
- Good luck!

- 5 marks 1. (*Keeping Both Eyes Open*) Let X , Y , and Z be discrete random variables with $I(X;Y) = 0$ and $I(X;Z) = 0$. An information theory student conjectures that it must be the case that $I(X;Y,Z) = 0$. Prove the conjecture or give a counterexample.
- 5 marks 2. (*Entropy Inequalities*) Let X_1, X_2, \dots be a stationary random process over a discrete alphabet. What are the general inequality relationships between the quantities $H(X_1)$, $H(X_2|X_1)$ and $\frac{1}{2}H(X_1, X_2)$? (Carefully justify each inequality.)
- 5 marks 3. (*Lempel-Ziv Parsing*)
- (a) Complete the Lempel-Ziv parsing into phrases of the following sequence:
- 0, 00, 001, 01111001010101.
- (b) Given an example of a sequence in which the Lempel-Ziv parsing gives phrases that are each as short as possible. What is the length (in bits) of the 100th such phrase?
- (c) Given an example of a sequence in which the Lempel-Ziv parsing gives phrases that are each as long as possible. What is the length (in bits) of the 100th such phrase?

10 marks 4. (*Entropy Bounds*) Let $p = (p_1, \dots, p_m)$ be the probability mass function for a random variable X defined on an alphabet of $m \geq 2$ letters.

(a) Suppose that $p_1 = 1/2$. Assuming $H(X)$ is measured in bits, show that

$$1 \leq H(X) \leq 1 + \frac{1}{2} \log_2(m - 1).$$

Show that these upper and lower bounds are tight in the sense that the upper bound is met with equality for some distribution with $p_1 = 1/2$, and similarly for the lower bound.

(b) Suppose that p_1 is some given value. Find general upper and lower bounds on $H(X)$ that are tight in the same sense as in part (a). (For $p_1 = 1/2$, your bounds should be the same as those of part (a).)

10 marks 5. (*Perfect Security*) In this problem we will consider the prospect of achieving perfectly secure communication between two parties who both have access to a common key (assumed unknown to any eavesdropper). Let X be an n -bit message drawn uniformly from the set $\{0, 1\}^n$, and let K be a k -bit key drawn uniformly from the set $\{0, 1\}^k$. Assume that K is independent of X . (The idea is that the key might be agreed upon before secure communication takes place, and so it should be independent of the message). A perfectly secure encryption scheme is a function f that takes in a message X and a key K to give a ciphertext $Y = f(X, K) \in \{0, 1\}^m$ with the properties that

$$\begin{aligned} I(X; Y) &= 0, \text{ i.e., lacking the key, the ciphertext gives no information} \\ &\quad \text{about the message; and} \\ H(X|Y, K) &= 0, \text{ i.e., given the ciphertext and the key, the message can} \\ &\quad \text{be recovered uniquely.} \end{aligned}$$

Show that in any such scheme we have $m \geq n$ and $k \geq n$, i.e., both the ciphertext and the key should have at least as many bits as the message. (*Optional*: describe a perfectly secure encryption scheme that achieves $m = k = n$.)

10 marks 6. (*Matching with Dyadic Distributions*) Recall that a distribution over a discrete alphabet is said to be *dyadic* if every probability mass is an integer power of $(1/2)$. Let $p = (p_1, \dots, p_m)$ be a given distribution. Describe an algorithm to determine a dyadic distribution $q = (q_1, \dots, q_m)$ that is a close match to p in the sense that $D(p||q)$ is minimal. Is there always a unique optimal dyadic distribution?