

# Information Theory

## Problem Sheet 1

(Most questions are from Cover & Thomas, the corresponding question numbers (as in 1<sup>st</sup> ed.) are given in brackets at the start of the question)

**Notation:**  $x$ ,  $\mathbf{x}$ ,  $\mathbf{X}$  are scalar, vector and matrix random variables respectively.

The following expressions may be useful:  $\sum_{n=1}^{\infty} r^n = \frac{r}{1-r}$   $\sum_{n=1}^{\infty} nr^n = \frac{r}{(1-r)^2}$

1. [2.1] A fair coin is flipped until the first head occurs. Let  $X$  denote the number of flips required.
  - (a) Find the entropy  $H(X)$  in bits.
  - (b) A random variable  $X$  is drawn according to this distribution. Find an “efficient” sequence of yes-no questions of the form “Is  $X$  contained in the set  $S$ ?”. Compare  $H(X)$  to the expected number of questions required to determine  $X$ .
2. [~2.2]  $X$  is a random variable taking integer values. What can you say about the relationship between  $H(X)$  and  $H(Y)$  if
  - (a)  $Y = X^2$
  - (b)  $Y = X^3$
3. [2.3] If  $\mathbf{p}$  is an  $n$ -dimensional probability vector, what is the maximum and the minimum value of  $H(\mathbf{p})$ . Find all vectors  $\mathbf{p}$  for which  $H(\mathbf{p})$  achieves its maximum or minimum value.

4. We write  $H(p)$  (with a scalar  $p$ ) to denote the entropy of the Bernoulli random variable with probability mass vector  $\mathbf{p} = [1-p \ p]$ . Prove the following properties of this function:
  - (a)  $H'(p) = \log(1-p) - \log p$
  - (b)  $H''(p) = \frac{-\log e}{p(1-p)}$
  - (c)  $H(p) \geq 2 \min(p, 1-p)$
  - (d)  $H(p) \geq 1 - 4(p - 1/2)^2$
  - (e)  $H(p) \leq 1 - 2 \log e (p - 1/2)^2$

5. [2.5] Let  $X$  be a discrete random variable and  $g(X)$  a deterministic function of it. Show that  $H(g(X)) \leq H(X)$  by justifying the following steps:
 
$$H(X, g(X)) \stackrel{(a)}{=} H(X) + H(g(X) | X) \stackrel{(b)}{=} H(X)$$

$$H(X, g(X)) \stackrel{(c)}{=} H(g(X)) + H(X | g(X)) \stackrel{(d)}{\geq} H(g(X))$$

6. [2.6] Show that if  $H(Y | X) = 0$ , then  $Y$  is a function of  $X$ , that is for all  $x$  with  $p(x) > 0$ , there is only one possible value of  $y$  with  $p(x, y) > 0$ .

7. [~2.7]  $x_i$  is a sequence of i.i.d. Bernoulli random variables with  $p(x_i=1) = p$  where  $p$  is unknown. We want to find a function  $f$  that converts  $n$  samples of  $x$  into a smaller number,  $K$ , of i.i.d. Bernoulli random variables,  $Z_i$ , with  $p(Z_i=1)=1/2$ . Thus  $Z_{1:K}=f(x_{1:n})$  where  $K$  can depend on the values  $x_i$ .

- (a) Show that the following mapping for  $n=4$  satisfies the requirements and find the expected value of  $K$ ,  $E(K)$ .

0000,1111 → ignore;      1010 → 0;      0101 → 1;      0001,0011,0111 → 00;  
0010,0110,1110 → 01;      0100,1100,1101 → 10;      1000,1001,1011 → 11

- (b) Justify the steps in the following bound on  $E(K)$

$$\begin{aligned} nH(p) &\stackrel{(a)}{=} H(x_{1:n}) \stackrel{(b)}{\geq} H(Z_{1:K}, K) \stackrel{(c)}{=} H(K) + H(Z_{1:K} | K) \\ &\stackrel{(d)}{=} H(K) + EK \stackrel{(e)}{\geq} EK \end{aligned}$$

8. [2.10] Give examples of joint random variables  $x, y$  and  $z$  such that:

- (a)  $I(x; y | z) < I(x; y)$   
(b)  $I(x; y | z) > I(x; y)$

9. [2.12] We can define the “mutual information” between three variables as

$$I(x; y; z) = I(x; y) - I(x; y | z)$$

- (a) Prove that

$$\begin{aligned} I(x; y; z) &= H(x, y, z) - H(x, y) - H(y, z) - H(z, x) \\ &\quad + H(x) + H(y) + H(z) \end{aligned}$$

- (b) Give an example where  $I(x; y; z)$  is negative. This lack of positivity means that it does not have the intuitive properties of an “information” measure which is why I put “mutual information” in quotes above.

10. [2.17] Show that  $\log_e(x) \geq 1-x^{-1}$  for  $x > 0$ .

11. [~2.16]  $x$  and  $y$  are correlated binary random variables with  $p(x=y=0)=0$  and all other joint probabilities equal to  $1/3$ . Calculate  $H(x)$ ,  $H(y)$ ,  $H(x|y)$ ,  $H(y|x)$ ,  $H(x, y)$ ,  $I(x, y)$ .

12. [~2.22] If  $x \rightarrow y \rightarrow z$  form a Markov chain, and for  $y$ , the alphabet size  $|Y| = k$ , show that  $I(x; z) \leq \log k$ . What does this tell you if  $k = 1$ ?

13. [2.29] Prove the following and find the conditions for equality:

- (a)  $H(x, y | z) \geq H(x | z)$   
(b)  $I(x, y; z) \geq I(x; z)$   
(c)  $H(x, y, z) - H(x, y) \leq H(x, z) - H(x)$   
(d)  $I(x, z | y) \geq I(z, y | x) - I(z, y) + I(x, z)$

# Information Theory

## Solution Sheet 1

1. (a)  $X = n$  means that Tail occurs for the first  $n - 1$  flips, while the last flip is Head. Thus,  $X$  has distribution  $P(X = n) = 2^{-(n-1)} 2^{-1} = 2^{-n}$ . Thus

$$\begin{aligned} H(X) &= \sum_{n=1}^{\infty} 2^{-n} \log 2^n = \sum_{n=1}^{\infty} 2^{-n} n \log 2 \\ &= \sum_{n=1}^{\infty} n 2^{-n} = \frac{1/2}{(1-1/2)^2} = 2 \end{aligned}$$

- (b) Ask if  $x = 1, 2, 3, \dots$  in turn, i.e., ask the following questions:

Is  $X = 1$ ?  
If not, is  $X = 2$ ?  
If not, is  $X = 3$ ?  
...

Expected number of questions is  $\sum_{n=1}^{\infty} n 2^{-n} = 2$ .

2.  $H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$ , but  $H(Y|X) = 0$  since  $Y$  is a function of  $X$  so  $H(Y) = H(X) - H(X|Y) \leq H(X)$  with equality iff  $H(X|Y) = 0$  which is true only if  $X$  is a function of  $Y$ , i.e. if  $Y$  is a one-to-one function of  $X$  for every value of  $x$  with  $p(x) > 0$ . Hence

- (a)  $H(Y) \leq H(X)$  because, for example  $1^2 = (-1)^2$

- (b)  $H(Y) = H(X)$

3. Maximum is  $\log n$  iff all elements of  $\mathbf{p}$  are equal. Minimum is 0 iff only one element of  $\mathbf{p}$  is non-zero; there are  $n$  possible elements that this could be.

4. (a) and (b) are straightforward calculus: easiest to convert logs to base  $e$  first. For the others, assume  $1/2 < p < 1$  for convenience (other half follows by symmetry). Since  $H''(p) < 0$ ,  $H(p)$  is concave and so lies above the straight line  $2 - 2p$  defined in (c).

At  $p = 1/2$  the bound in (e) has the same value and first two derivatives as  $H(p)$ . For  $1/2 < p < 1$  its second derivative is greater than  $H''(p)$  and so the bound follows.

For (d) we consider  $D(p) = H(p) - 1 + 4(p - 1/2)^2$ .  $D''(p) = 0$  is a quadratic in  $p$  and has only two solutions  $p = 1/2 \pm \sqrt{(2 - \log e)/8} = 0.5 \pm 0.26$ . Therefore  $D'(p)$  increases from 0 at  $p = 0.5$  to reach a maximum at  $p = 0.76$  and decreases thereafter. This implies that  $D'(p) = 0$  has only one solution for  $p > 1/2$  and therefore that  $D(p)$  has a single maximum. Since  $D(1/2) = D(1) = 0$  we must have  $D(p) > 0$  for  $1/2 < p < 1$ .

5. (a) chain rule, (b)  $g(X)|X$  has only one possible value and hence zero entropy, (c) chain rule, (d) entropy is positive. We have equality at (d) iff  $g(X)$  is a one-to-one function for every  $x$  with  $p(x) > 0$ .

6.  $H(Y|X) = \sum_x p(x) H(Y|X = x)$

All terms are non-negative so the sum is zero only if all terms are zero. For any given term this is true either if  $p(x) = 0$  or if  $H(Y|X=x)$  is zero. The second case arises only if  $H(Y|X=x)$  has only one value, i.e.  $Y$  is a function of  $X$ . The first case is why we needed the qualification about  $p(x) > 0$  in answers 2 and 4 above.

7. (a) The probability of any given value of  $X_{1:4}$  depends on the number of 1's and 0's. We create four subsets with equal probabilities to generate a pair of bits and two other subsets to generate one bit only. The expected number of bits generated is

$$EK = 8p(1-p)^3 + 10p^2(1-p)^2 + 8p^3(1-p)$$

- (b) (a) i.i.d entropies add, (b) functions reduce entropy, (c) chain rule, (d)  $Z_i$  are i.i.d. with entropy of 1 bit, (e) entropy is positive.

8. (a) This is true for any Markov chain  $X \rightarrow Y \rightarrow Z$ . One possibility is  $X=Y=Z$  all fair Bernoulli variables.

- (b) An example of this was given in lectures. A slightly different example is if  $X$  and  $Y$  are fair binary variables and  $Z = XY$ . Knowing  $Z$ , entangles  $X$  and  $Y$ .

9. (a)  $I(X, Y, Z) = \{H(X) - H(X|Y)\} - \{H(X|Z) - H(X|Y, Z)\} = H(X) - \{H(X, Y) - H(Y)\} - \{H(X, Z) - H(Z)\} + \{H(X, Y, Z) - H(Y, Z)\}$

- (b) Use the example from 8(b) above.

10. Define  $f(x) = \ln(x) + x^{-1} - 1$ . This is continuous and differentiable in  $(0, \infty)$ . Differentiate twice to show that the only extremum occurs at  $x=1$  and that it is a minimum. Hence  $f(x) \geq f(1) = 0$ .
11.  $H(x) = H(y) = 0.918$ ;  $H(x|y) = H(y|x) = 0.667$ ;  $H(x, y) = 1.58$ ;  $I(x, y) = 0.252$ .
12. The data processing inequality says that  $I(x, z) \leq I(x, y) = H(y) - H(y|x) \leq H(y) \leq \log k$  where the last inequality is the uniform bound on entropy. If  $k=1$  then  $\log k = 0$  and so  $x$  and  $z$  must be independent.
13. (a)  $H(x, y|z) = H(x|z) + H(y|x, z) \geq H(x|z)$  with equality if  $y$  is a function of  $x$  and  $z$ .
- (b)  $I(x, y, z) = I(x, z) + I(y, z|x) \geq I(x, z)$  with equality if  $y$  and  $z$  are conditionally independent given  $x$ .
- (c)  $H(x, y, z) - H(x, y) = H(z|x, y) = H(z|x) - I(y, z|x) \leq H(z|x) = H(x, z) - H(x)$  with equality if  $y$  and  $z$  are conditionally independent given  $x$ .
- (d)  $I(x, y, z) = I(y, z) + I(x, z|y) = I(x, z) + I(y, z|x)$ . Rearrange this to give the inequality which is in fact always an equality (trick question).

# Information Theory

## Problem Sheet 2

**Notation:**  $x$ ,  $\mathbf{x}$ ,  $\mathbf{X}$  are scalar, vector and matrix random variables respectively.

- Use the Kraft inequality to show that it is possible to construct a 4-ary instantaneous code with lengths  $\{1, 1, 2, 2, 2, 2, 2, 2\}$ . Construct such a code for symbols that take the values A, B, ..., H, I with probabilities  $\{.15, .15, .1, .1, .1, .1, .1, .1\}$ .

Calculate the entropy of the input symbols and the expected length of the codewords.

- The four symbols A, B, C, D are encoded using the following sets of codewords. In each case state whether the code is (i) non-singular, (ii) uniquely decodable and (iii) instantaneous code.

- $\{1, 01, 000, 001\}$
- $\{0, 10, 000, 100\}$
- $\{01, 01, 110, 100\}$
- $\{0, 01, 011, 0111\}$
- $\{10, 01, 0010, 0111\}$

01

- In a complete  $D$ -ary code tree, the end of each branch is either a leaf node or else has  $D$  sub-branches. Show that the total number of leaf nodes is one more than a multiple of  $D-1$ .

- For each value of  $D$  given below, find a  $D$ -ary Huffman code for the probability vector  $\{0.25, 0.2, 0.15, 0.1, 0.1, 0.1, 0.1\}$ . In each case calculate the expected code length. [Note that, to ensure a full code tree, you should add zero-probability symbols so that the total number of symbols is one more than a multiple of  $D-1$ ]

- $D = 3$
- $D = 4$
- $D = 5$

- Find a binary instantaneous code with codeword lengths  $\{2, 2, 3, 3, 3, 4, 4\}$ . Find a probability mass vector for which the expected length of this code is equal to the entropy of the source.

- [4.2] If  $\{X_i\}$  is a stationary stochastic process, show that

$$H(X_i | X_{i-1}, X_{i-2}, \dots, X_{i-n}) = H(X_i | X_{i+1}, X_{i+2}, \dots, X_{i+n}).$$

In other words, the conditional entropy given the previous  $n$  samples is the same as the conditional entropy given the next  $n$  samples.

- (a) [4.5] Determine the stationary distribution and the entropy rate,  $H(X)$ , of a Markov process with two states, 0 and 1 and transition matrix

$$T = \begin{pmatrix} 1-p & p \\ q & 1-q \end{pmatrix}.$$

- Find the values of  $p$  and  $q$  that maximize  $H(X)$ .
- If  $q=1$ ,
  - find the maximum value of  $H(X)$  and the value of  $p$  that attains it.
  - define  $s(n)$  to be the number of sequences of length  $n$  with non-zero probability. If  $s_0(n)$  and  $s_1(n)$  are the number of sequences starting with 0 and 1 respectively, show that  $s_1(n) = s_0(n-1) = s(n-2)$ . Hence show that  $s(n) = s(n-1) + s(n-2)$  and derive an explicit expression for  $s(n)$ .
  - explain why we must have  $H(X) \leq \lim_{n \rightarrow \infty} (n^{-1} \log s(n))$  and calculate the value on the right hand side.

- If  $X_i \in \{A, B\}$  are i.i.d. with probability mass vector  $\{0.9, 0.1\}$ , determine  $H(X_i)$ .

Using binary Huffman codes, determine the coding redundancy (i.e. the difference between the entropy and the number of bits used per symbol) when (a) each  $X_i$  is encoded individually, (b) pairs of  $X_i$  are coded together (i.e.  $X_1X_2$  followed by  $X_3X_4$  etc) and (c) triplets of  $X_i$  are coded together.

# Information Theory

## Solution Sheet 2

1. Kraft Inequality:  $2 \times 4^{-1} + 7 \times 4^{-2} = 0.9375 \leq 1$  so an instantaneous code is possible. A suitable code is {0, 1, 20, 21, 22, 23, 30, 31, 32}.  
Average length of code is 1.7 (equivalent to 3.4 bits since we are using a 4-ary code).  
Entropy of input is 3.1464 bits.
2. Note that Instantaneous  $\Rightarrow$  Uniquely Decodable  $\Rightarrow$  Non-singular
  - (a) {1, 01, 000, 001} is an instantaneous code (and therefore uniquely decodable and non-singular).
  - (b) {0, 10, 000, 100} is non-singular since no two codewords are the same. However it is not uniquely decodable since AAA and C are indistinguishable (it follows that it is not an instantaneous code either).
  - (c) {01, 01, 110, 100} is singular since A and B have the same codeword (hence not uniquely decodable and not an instantaneous code).
  - (d) {0, 01, 011, 0111} is uniquely decodable: when you get a 0 it is the start of a new symbol and the previous symbol is given by counting how many 1's since the previous 0. It is not an instantaneous code since the first codeword is a prefix of all the others.
  - (e) {10, 01, 0010, 0111} is not an instantaneous code since 01 is a prefix of 0111. Since all codewords have even length we can rewrite it as a 4-ary code {2, 1, 02, 13}. It is easy to see that this is uniquely decodable since 3 only ever appears as the second half of D. Thus if a 1 is followed by anything other than 3, it represents a B.
3. You can create the tree incrementally from an initial tree with only one node. At each stage, you replace an existing leaf node with a set of  $D$  sub-branches which end in leaf nodes. This process adds  $D$  new leaf nodes but removes one that existed previously. It therefore adds  $D-1$  to the total. Initially, we only had one leaf node and so we will always have one more than a multiple of  $D-1$ .
4. (a)  $D = 3$ . We do not need to append any zero-probability symbols since 7 is one more than a multiple of  $D-1$  already. The codes we get are {2, 00, 01, 02, 10, 11, 12}. The expected length is 1.75.

- (b)  $D = 4$ . Again 7 is one more than a multiple of  $D-1$  so we do not need to add any symbols. The codes we get are {1, 2, 3, 00, 01, 02, 03}. The expected length is 1.4.
- (c)  $D = 5$ . We need two zero-probability symbols to make the number of symbols one more than a multiple of 4. The codes we get are then {1, 2, 3, 4, 00, 01, 02, [03, 04]} where the last two codes are in brackets because they are not used. Not that adding the zero-probability symbols ensures that the unused codes are the longest ones. The expected length is now 1.3.

5. A suitable code is {00, 01, 100, 101, 110, 1110, 1111}.

To attain the source entropy, all the symbol probabilities must equal  $2^{-l}$ . This gives us {0.25, 0.25, 0.125, 0.125, 0.125, 0.0625, 0.0625} as the probabilities.

6. We can write the following:

$$\begin{aligned}
 H(X_i | X_{i-1}, X_{i-2}, \dots, X_{i-n}) &\stackrel{(a)}{=} H(X_i, X_{i-1}, X_{i-2}, \dots, X_{i-n}) - H(X_{i-1}, X_{i-2}, \dots, X_{i-n}) \\
 &\stackrel{(b)}{=} H(X_{i+n}, X_{i+n-i}, X_{i+n-2}, \dots, X_i) - H(X_{i+n}, X_{i+n-1}, \dots, X_{i+1}) \\
 &\stackrel{(c)}{=} H(X_i | X_{i+1}, X_{i+2}, \dots, X_{i+n})
 \end{aligned}$$

Where (a) and (c) follow from the definition of conditional entropy and (b) follows from stationarity: we add  $n$  onto the time index of the first term and  $n+1$  onto the time index of the second.

7. (a) To find the stationary distribution, we write

$$\begin{aligned}
 T^T \begin{pmatrix} a \\ 1-a \end{pmatrix} &= \begin{pmatrix} 1-p & q \\ p & 1-q \end{pmatrix} \begin{pmatrix} a \\ 1-a \end{pmatrix} = \begin{pmatrix} a \\ 1-a \end{pmatrix} \\
 \Rightarrow (1-p)a + q(1-a) &= (1-p-q)a + q = a \\
 \Rightarrow a &= q(p+q)^{-1}
 \end{aligned}$$

It follows that the entropy rate is given by

$$H(X) = aH(p) + (1-a)H(q) = (qH(p) + pH(q))(p+q)^{-1}$$

This is a weighted average of  $H(p)$  and  $H(q)$  with the weights equal to their frequencies in the stationary distribution.

- (b) We know that  $H(X) = H(X_n | X_{n-1}) \leq H(X_n) \leq 1$

If  $p = q = 0.5$  then  $H(X) = H(p) = H(q) = 1$  and this is the maximum attainable.

- (c-i) Substituting  $q = 1$  into the previous answer gives  $H(X) = (p+1)^{-1}H(p)$ . Differentiating and setting this to zero gives  $H(p) = (p+1)H'(p)$  from which we get  $p = (1-p)^2$  and  $p = 1.5 - \sqrt{1.25} = 0.382$ . This gives  $H(X) = 0.694$  bits.

- (c-ii) If the first bit is 0 the next can be either 0 or 1 which means that  $s_0(n) = s(n-1)$ . However  $q = 1$ , if the first bit of a sequence is 1, then the next must be 0. It follows that  $s_1(n) = s_0(n-1) = s(n-2)$ . Hence  $s(n) = s_0(n) + s_1(n) = s(n-1) + s(n-2)$  with the initial conditions  $s(1) = 2$  and  $s(2) = 3$ . The solutions to the recurrence relation (which is that of the Fibonacci series for those interested in such things) have the form  $s(n) = a^n$  where  $a$  satisfies  $a^2 = a + 1 \Rightarrow a = 0.5 \pm \sqrt{1.25} = \{-0.618, 1.618\}$ . Imposing the initial conditions gives  $s(n) = -0.17 \times -0.618^n + 1.17 \times 1.618^n$ . For large  $n$ , the first term is insignificant and  $s(n) \approx 1.17 \times 1.618^n$ .

- (c-iii) By definition  $H(X) = \lim_{n \rightarrow \infty} (n^{-1}H(X_{1:n}))$ . An upper bound on  $H(X_1, X_2, \dots, X_n)$  is given by  $\log s(n)$  which is attained if all  $s(n)$  possible sequences have equal probability. Thus  $\lim_{n \rightarrow \infty} (n^{-1} \log s(n)) = \log 1.618 = 0.694$  is an upper bound for  $H(X)$ .

8.  $H(X_i) = 0.469$  bits.

- (a)  $p\{A, B\} = \{0.9, 0.1\}$  giving Huffman lengths of  $\{1, 1\}$  with  $E(L) = 1$ . Redundancy = 0.531 bits.
- (b)  $p\{AA, AB, BA, BB\} = \{0.81, 0.09, 0.09, 0.01\}$  giving Huffman lengths of  $\{1, 2, 3, 3\}$  with  $E(L)/2 = 1.29/2 = 0.645$  bits per input symbol. Redundancy = 0.176 bits.
- (c)  $p\{AAA, AAB, ABA, BAA, ABB, BAB, BBA, BBB\} = \{0.729, 0.081 \times 3, 0.009 \times 3, 0.001\}$  giving Huffman lengths of  $\{1, 3, 3, 3, 5, 5, 5, 5\}$  with  $E(L)/3 = 1.598/3 = 0.533$  bits per input symbol. Redundancy = 0.064 bits.

# Information Theory

## Problem Sheet 3

**Notation:**  $X$ ,  $\mathbf{x}$ ,  $\mathbf{X}$  are scalar, vector and matrix random variables respectively.

1. The Z channel. The Z-channel has binary input and output alphabets and transition probabilities  $p(y|x)$  given by the following matrix:

$$Q = \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \end{bmatrix} \quad x, y \in \{0,1\}$$

Find the capacity of the Z-channel and the maximizing input probability distribution.

2. Calculate the capacity of the following channel with probability transition matrix

$$Q = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \end{bmatrix} \quad x, y \in \{0,1,2\}$$

3. Differential entropy. Evaluate the differential entropy  $h(X) = -\int f \ln f$  for the following:
  - (a) The exponential density  $f(x) = \lambda e^{-\lambda x}$ ,  $x \geq 0$ .
  - (b) The sum of  $X_1$  and  $X_2$ ; where  $X_1$  and  $X_2$  are independent normal random variables with means  $\mu_i$  and variances  $\sigma_i^2$  for  $i = 1, 2$ .

4. Parallel channels and waterfilling. Consider a pair of parallel Gaussian channels, i.e.,

$$\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} + \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix}$$

where

$$\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} \sim N\left(0, \begin{bmatrix} \sigma_1^2 & 0 \\ 0 & \sigma_2^2 \end{bmatrix}\right)$$

and there is a power constraint  $E(X_1^2 + X_2^2) \leq 2P$ . Assume that  $\sigma_1^2 \geq \sigma_2^2$ . At what power does the channel stop behaving like a single channel with noise variance  $\sigma_2^2$  and begin behaving like a pair of channels?

5. Rate-distortion function. Let

$$D(R) = \min_{p(\hat{x}|x): I(X; \hat{X}) \leq R} Ed(X, \hat{X})$$

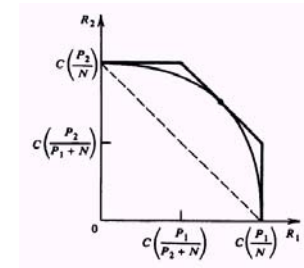
be the rate-distortion function.

- (a) Is  $D(R)$  a decreasing or increasing function of  $R$ ?
- (b) Is  $D(R)$  convex or concave in  $R$ ?

6. Describe the capacity region of a two-user multiple access channel. Interpret the corner points (i.e., why can one of the users achieve the capacity as if the other user were absent?) Verify the following equality for the corner point:

$$C\left(\frac{P_1}{N}\right) + C\left(\frac{P_2}{P_1 + N}\right) = C\left(\frac{P_1 + P_2}{N}\right)$$

where  $C(x) = (\log(1+x))/2$  is the capacity function.



7. Slepian-Wolf region for binary sources. Let  $X_i$  be i.i.d. Bernoulli( $p$ ). Let  $Z_i$  be i.i.d. Bernoulli( $r$ ), and let  $Z$  be independent of  $X$ . Finally, let  $Y = X \oplus Z$  (mod 2 addition). Let  $X$  be described at rate  $R_1$  and  $Y$  be described at rate  $R_2$ : What region of rates allows recovery of  $X$ ,  $Y$  with probability of error tending to zero?
8. Describe the capacity region of a two-user Gaussian broadcast channel and sketch it.



# Information Theory

## Solution Sheet 3

1. First we express  $I(X;Y)$ , the mutual information between the input and output of the Z-channel, as a function of  $x = \Pr(X = 1)$ :

$$H(Y|X) = P(X = 0) \cdot 0 + P(X = 1) \cdot 1 = x$$

$$H(Y) = H(P(Y = 1)) = H(x/2)$$

$$I(X;Y) = H(Y) - H(Y|X) = H(x/2) - x$$

Taking the derivative, we have

$$\frac{dI(X;Y)}{dx} = \frac{1}{2} \log_2 \frac{1-x/2}{x/2} - 1$$

which is equal to zero for  $x = 2/5$ . So the capacity of the Z-channel in bits is  $H(1/5) - 2/5 = 0.722 - 0.4 = 0.322$ .

2. Since the channel is symmetric,

$$C = \log |Y| - H(Q(1,:)) = \log_2 3 - 1 = 0.58 \text{ bits}$$

3. (a)  $\log(e/\lambda)$  bits.

$$\begin{aligned} h(X) &= -\int_0^\infty f(x) \log f(x) dx = -\log e \int_0^\infty f(x) \ln f(x) dx \\ &= -\log e \int_0^\infty \lambda e^{-\lambda x} (\ln \lambda - \lambda x) dx = -\log e (\ln \lambda - \int_0^\infty \lambda x e^{-\lambda x} d\lambda x) \\ &= -\log e (\ln \lambda - 1) = -\log e \cdot \ln(\lambda/e) = \log(e/\lambda) \text{ bits} \end{aligned}$$

- (b) The sum of two normal random variables is also normal, so applying the result derived the class for the normal distribution,

$$h(f) = \frac{1}{2} \log 2\pi e(\sigma_1^2 + \sigma_2^2) \text{ bits}$$

4. By the result of Lecture 14, it follows that we will put all the signal power into the channel with less noise until the total power of noise + signal in that channel equals the noise power in the other channel. After that, we will split any additional power “evenly” (in the sense that the power of noise + signal in one channel is equal to that in the other channel) between the two channels. Thus the combined channel begins to

behave like a pair of parallel channels when the signal power is equal to the difference of the two noise powers, i.e., when  $2P = \sigma_1^2 - \sigma_2^2$ .

5. (a) Decreasing.  
(b) Convex.  
6. Capacity region

$$R_1 < C\left(\frac{P_1}{N}\right)$$

$$R_2 < C\left(\frac{P_2}{N}\right)$$

$$R_1 + R_2 < C\left(\frac{P_1 + P_2}{N}\right)$$

Interpretation: onion-peeling.

Verification:

$$\begin{aligned} C\left(\frac{P_1 + P_2}{N}\right) &= \frac{1}{2} \log\left(1 + \frac{P_1 + P_2}{N}\right) \\ &= \frac{1}{2} \log\left(\frac{N + P_1 + P_2}{N}\right) \\ &= \frac{1}{2} \log\left(\frac{N + P_1 + P_2}{N + P_1} \cdot \frac{N + P_1}{N}\right) \\ &= \frac{1}{2} \log\left(\frac{N + P_1 + P_2}{N + P_1}\right) + \frac{1}{2} \log\left(\frac{N + P_1}{N}\right) \\ &= C\left(\frac{P_2}{P_1 + N}\right) + C\left(\frac{P_1}{N}\right) \end{aligned}$$

7. The Slepian-Wolf region is given by

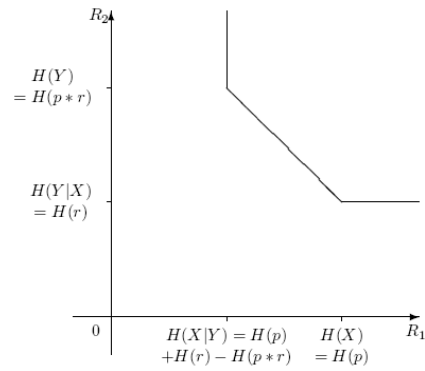
$$R_1 \geq H(X|Y)$$

$$R_2 \geq H(Y|X)$$

$$R_1 + R_2 \geq H(X, Y)$$

$X = \text{Bernoulli}(p)$ ,  $Y = X \oplus Z$ ,  $Z = \text{Bernoulli}(r)$ . Then  $Y = \text{Bernoulli}(p^*r)$ , where  $p^*r = p(1-r) + r(1-p)$ .  $H(X) = H(p)$ ,  $H(Y) = H(p^*r)$ ,  $H(X, Y) = H(X, Z) = H(X) + H(Z) = H(p) + H(r)$ . Hence  $H(Y|X) = H(r)$  and  $H(X|Y) = H(p) + H(r) - H(p^*r)$ .

This region is shown in the next page.



8. The capacity region is

$$R_1 \leq C\left(\frac{\alpha P}{N_1}\right)$$

$$R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + N_2}\right)$$

where  $0 \leq \alpha \leq 1$ . It looks like this:

