Dr R Venkataramanan

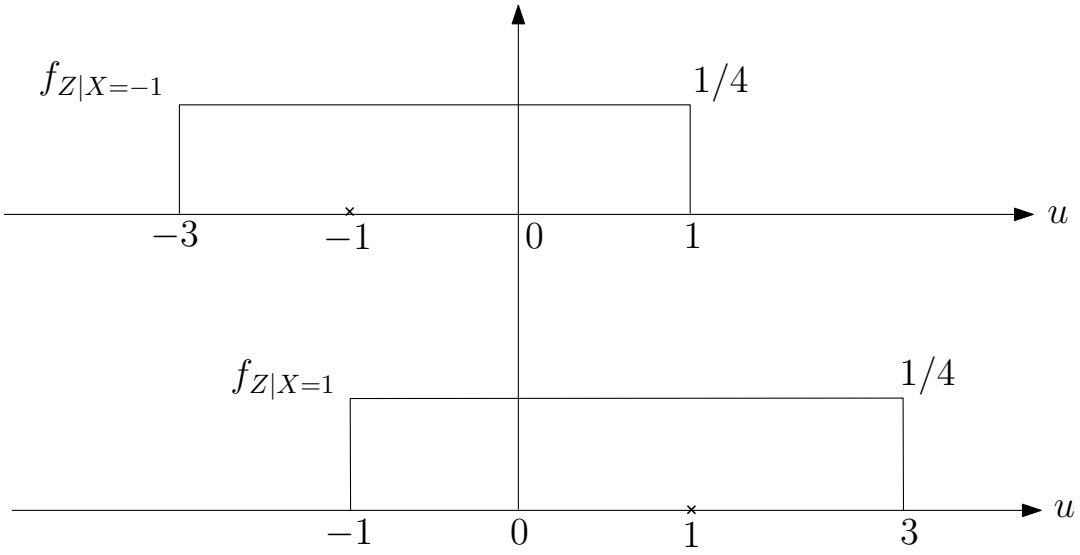
4F5 Advanced Communications and Coding Engineering Tripos 2013/14 – Solutions

Question 1

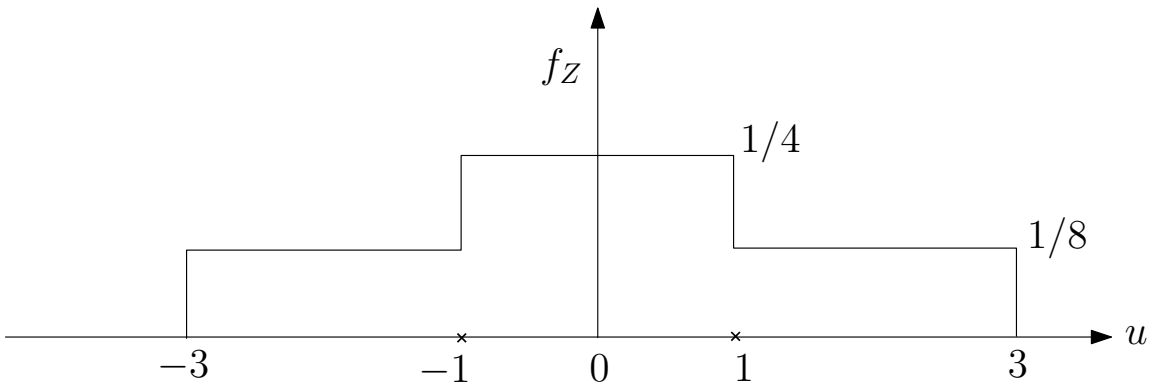
(a) i) Using the law of total probability, the pdf of Z, denoted f_Z, can be computed as

$$\begin{aligned} f_Z(u) &= P(X=1) f_{Z|X=1}(u) + P(X=-1) f_{Z|X=-1}(u) \\ &= \frac{1}{2} f_{Z|X=1}(u) + \frac{1}{2} f_{Z|X=-1}(u). \end{aligned} \tag{1}$$

As $Z = X + Y$ and $Y \sim Unif[-2, 2]$, the conditional pdfs $f_{Z|X=-1}$ and $f_{Z|X=1}$ are as shown below



Therefore, from (1), the pdf f_z is the following: [25%]



ii) The differential entropy of Z is

$$\begin{aligned} h(Z) &= \int_{-3}^{3} f_Z(u) \log \frac{1}{f_Z(u)} du \\ &= \int_{-3}^{-1} \frac{1}{8} \log 8 \, du + \int_{-1}^{1} \frac{1}{4} \log 4 \, du + \int_{1}^{3} \frac{1}{8} \log 8 \, du = \frac{3}{4} + 1 + \frac{3}{4} = 2.5 \text{ bits.} \end{aligned}$$

[15%]

(b) Consider $H(X, Y|X+Y)$, the joint entropy of (X, Y) conditioned on $X+Y$. Using the chain rule, we have

$$H(X, Y|X+Y) = H(X|X+Y) + \underbrace{H(Y|X+Y,\, X)}_{0} = H(X|X+Y) \tag{2}$$

where $H(Y|X+Y,\, X) = 0$ because Y is a deterministic function of $(X, X+Y)$. Similarly, using the chain rule in a different order we get

$$H(X, Y|X+Y) = H(Y|X+Y) + \underbrace{H(X|X+Y,\, Y)}_{0} = H(Y|X+Y). \tag{3}$$

(2) and (3) imply that [25%]

$$H(X|X+Y) = H(Y|X+Y).$$

(c) We have

$$I(X;Y) = H(X) - H(X|Y) \leq H(X) \leq \log M. \tag{4}$$

where the first inequality holds because conditioning cannot increase entropy, and the second inequality holds because the entropy of a random variable is upper bounded by the log of the alphabet size.

Similarly,

$$I(X;Y) = H(Y) - H(Y|X) \leq H(X) \leq \log N. \tag{5}$$

From (4) and (5), we conclude that

$$I(X;Y) \leq \min\{\log M, \log N\}. \tag{6}$$

Therefore capacity of a discrete memoryless channel with input X and output Y is given by [35%]

$$\mathcal{C} = \max_{P_X} I(X;Y) \leq \min\{\log M, \log N\}$$

Question 2

(a) *Find an element β of multiplicative order 6 in GF(7). What is the value and the multiplicative order of $\alpha = \beta^2$?*

$\beta = 3$ has multiplicative order 6 in GF(7) because [10%]

$$\beta^1 = 3, \beta^2 = 2, \beta^3 = 6, \beta^4 = 4, \beta^5 = 5, \beta^6 = 1.$$

$\alpha = \beta^2 = 2$ has multiplicative order 3.

(b) *Specify a 2×3 parity-check matrix for the Reed Solomon code of length 3 over GF(7). What is the code dimension? Is the parity-check matrix unique?*

The parity-check matrix is obtained from retaining the first two rows of the DFT matrix, i.e., [20%]

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}.$$

The code has dimension 1 (code length 3 minus the number of parity check equations 2). The parity-check matrix is not unique as any other basis of the dual code is a parity-check matrix for the same code. For example, we can use Gaussian elimination on the rows to get another parity check matrix for the same code.

(c) *Specify an encoding matrix for the code. How many codewords does the code contain?*

The parity-check matrix can be brought into systematic form $[-P^T; I]$ by Gaussian elimination to yield [15%]

$$\mathbf{H}_{\text{sys}} = \begin{bmatrix} 5 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}$$

hence the corresponding systematic encoding matrix of the form $[I; P]$ can be obtained as

$$\mathbf{G}_{\text{sys}} = \begin{bmatrix} 1 & 2 & 4 \end{bmatrix}.$$

The code contains 7 codewords — these are obtained by multiplying $\mathbf{G}_{\text{sys}}$ with the symbols $0, 1, \ldots, 6$.

(d) *A codeword has been transmitted over a noisy channel and the corresponding received vector is $\mathbf{r} = [2, 0, 1]$. Assume that the channel causes at most one error over a block of 3 code symbols.*

i) *Define the linear complexity of a finite length sequence.*

The linear complexity of a finite length sequence is the length of the shortest linear feedback shift register (LFSR) that generates the sequence irrespective of what follows. [10%]

ii) *What is the linear complexity of the DFT of the error sequence? Justify your answer.*

By multiplying the received sequence by the parity-check matrix

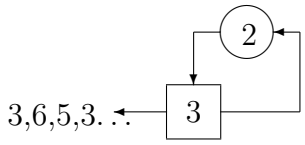
$$[2, 0, 1] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}^T = [3, 6],$$

we note that the received sequence is not a codeword since we would otherwise have obtained a syndrome $[0, 0]$ rather than $[3, 6]$. Hence, we conclude that there have been

transmission errors in the channel, and since we are told that the channel makes at most one error, we know that the Hamming weight of the error sequence is exactly one. By Blahut's theorem, the linear complexity of the DFT of the error sequence is equal to the Hamming weight of the sequence itself, hence its linear complexity is 1. [15%]

iii) *Find the shortest Linear Feedback Shift Register (LFSR) that generates the DFT of the error sequence.*

The LFSR is illustrated below. [10%]



iv) *Use the LFSR and the inverse DFT to recover the error sequence in the time domain.*

The complete error sequence in the frequency domain is $[3, 6, 5]$. We multiply by the inverse DFT matrix to obtain the error sequence in the time domain [10%]

$$\mathbf{e} = [3, 6, 5] \begin{bmatrix} 5 & 5 & 5 \\ 5 & 6 & 3 \\ 5 & 3 & 6 \end{bmatrix} = [0, 3, 0].$$

v) *Determine the transmitted codeword.*

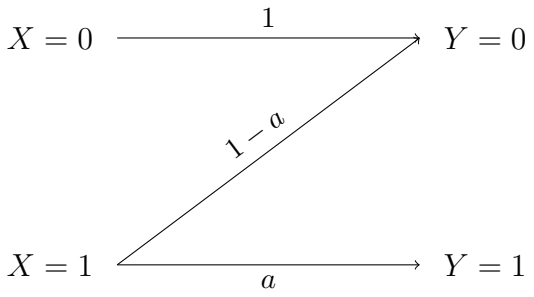
The transmitted codeword is the received word minus the error sequence, i.e.,

$$\mathbf{c} = \mathbf{r} - \mathbf{e} = [2, 0, 1] - [0, 3, 0] = [2, 4, 1].$$

It is easy to verify by multiplying the result by $\mathbf{H}^T$ that this is indeed a codeword of our Reed Solomon code. [10%]

Question 3

(a) i) The channel is depicted in the figure below.



Let the input distribution be $P(X = 1) = p$ and $P(X = 0) = 1 - p$. The distribution of Y is then

$$P(Y = 1) = pa, \quad P(Y = 0) = 1 - pa. \tag{7}$$

The mutual information can be expressed as

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &= H_2(ap) - H(Y|X) \\ &= H_2(ap) - [(1-p)H(Y|X=0) + pH(Y|X=1)] \\ &= H_2(ap) - pH_2(a). \end{aligned} \tag{8}$$

To find the capacity, we need to optimise over p. The derivative of $I(X;Y)$ with respect to p is [40%]

$$\frac{d}{dp} I(X;Y) = a \log_2 \left(\frac{1-ap}{ap} \right) - H_2(a). \tag{9}$$

Setting (9) to 0 and solving for p yields the optimum value

$$p^* = \frac{1}{a(2^{H_2(a)/a} + 1)}.$$

It is easily verified that the second derivative is always negative and so p^* attains the maximum. Substituting the value of p^* into (8) and simplifying yields the capacity

$$\mathcal{C} = \log_2 \left(2^{H_2(a)/a} + 1 \right) - \frac{H_2(a)}{a}. \tag{10}$$

ii) For $a = \frac{1}{2}$, $p^* = \frac{2}{5}$ and $\mathcal{C} = 0.3219$. (This is the Z-channel from Examples Paper 1).

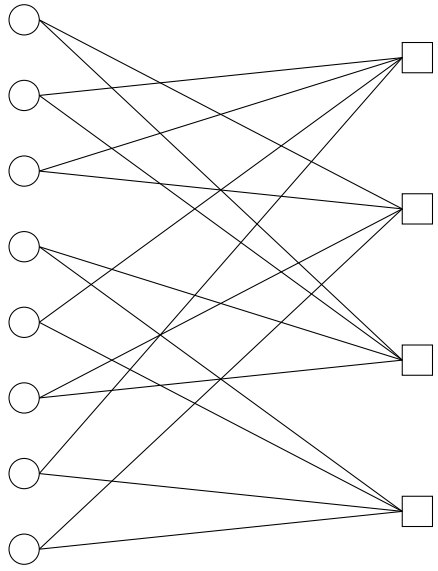
Fix a rate $R < \mathcal{C}$ and a sufficiently large block length n. Construct a codebook of 2^{nR} length-n codewords with each symbol of each codeword generated i.i.d according to $P_X(0) = 3/5, P_X(1) = 2/5$. [25%]

A joint typicality decoder can be used to recover the transmitted codeword with arbitrarily low probability of error by taking sufficiently large n.

(b) The parity check matrix is

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

i) The factor graph is drawn below. [15%]



ii) The solution is best illustrated by writing the received vector under the parity-check matrix as follows [20%]

$$\left[\begin{array}{cccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & \epsilon & \epsilon & 0 & 0 & 1 & \epsilon \end{array}\right]$$

We note that the first parity-check equation involves only the first of the 3 erasures, resolving it as 1. The third parity-check equation involves only the second of the 3 erasures, resolving it as 1. The third of the 3 erasures can now be resolved using either equation 2 or 4, and its value is 0. Hence the transmitted codeword is $[1, 0, 1, 1, 0, 0, 1, 0]$.

Question 4

(a) i) $E_s = \frac{1}{3}((-A)^2 + 0 + A^2) = \frac{2A^2}{3}$. [10%]

ii) As all the symbols are equally likely, the optimal MAP detector reduces to the minimum distance rule:

$$\hat{X} = \underset{X\in\{-A,0,A\}}{\arg\max}\ P(X)f(Y|X) = \underset{X\in\{-A,0,A\}}{\arg\max}\ f(Y|X) = \underset{X\in\{-A,0,A\}}{\arg\min}\ (Y-X)^2.$$

(Here $f(Y|X)$ is the pdf of the output given input X. It is $\mathcal{N}(X, \frac{N_0}{2})$.)
The decision regions are [15%]

$$\hat{X} = \begin{cases} A & \text{if } Y \le -A/2 \\ 0 & \text{if } -A/2 < Y < A/2 \\ A & \text{if } Y \ge A/2 \end{cases}$$

iii) The probability of error is

$$\begin{aligned} &P(\hat{X} \neq X) \\ &= P(X=A)P(\hat{X}\neq A|X=A) + P(X=0)P(\hat{X}\neq 0|X=0) \\ &\quad + P(X=-A)P(\hat{X}\neq A|X=-A) \\ &= \frac{1}{3}[P(\hat{X}\neq A|X=A) + P(\hat{X}\neq 0|X=0) + P(\hat{X}\neq A|X=-A)] \end{aligned} \tag{11}$$

For $X=0$, we have

$$\begin{aligned} P(\hat{X}\neq 0 \mid X=0) &= P(\{Y \le -\tfrac{A}{2}\} \cup \{Y > +\tfrac{A}{2}\} \mid X=0) \\ &= P(\{0+N \le -\tfrac{A}{2}\} \cup \{0+N > \tfrac{A}{2}\} \mid X=0) \\ &= P\left(\left\{ \frac{N}{\sqrt{N_0/2}} \le -\frac{A/2}{\sqrt{N_0/2}} \right\} \cup \left\{ \frac{N}{\sqrt{N_0/2}} > \frac{A/2}{\sqrt{N_0/2}} \right\} \right) \\ &= 2\mathcal{Q}\left(\sqrt{\frac{A^2}{2N_0}} \right). \end{aligned} \tag{12}$$

For $X=A$, we have [25%]

$$\begin{aligned} P(\hat{X}\neq A \mid X=A) &= P(\{Y < \tfrac{A}{2}\} \mid X=A) \\ &= P(\{A+N < \tfrac{A}{2}\} \mid X=A) = P(\{N < -\tfrac{A}{2}\}) = \mathcal{Q}\left(\sqrt{\frac{A^2}{2N_0}} \right). \end{aligned} \tag{13}$$

By symmetry, $P(\hat{X}\neq -A \mid X=-A)$ is also equal to $\mathcal{Q}\left(\sqrt{\frac{A^2}{2N_0}}\right)$. Therefore, from (11) the overall probability of error for the constellation is

$$\begin{aligned} P(\hat{X}\neq X) &= \frac{1}{3}\left(\mathcal{Q}\left(\sqrt{\tfrac{A^2}{2N_0}}\right) + 2\mathcal{Q}\left(\sqrt{\tfrac{A^2}{2N_0}}\right) + \mathcal{Q}\left(\sqrt{\tfrac{A^2}{2N_0}}\right)\right) \\ &= \frac{4}{3}\mathcal{Q}\left(\sqrt{\tfrac{A^2}{2N_0}}\right) = \frac{4}{3}\mathcal{Q}\left(\sqrt{\tfrac{3E_s}{4N_0}}\right) \end{aligned} \tag{14}$$

where the last equality is obtained using $E_s = 2A^2/3$.

(b) i) Multiplying the output by $h^*/|h|$, we obtain

$$\bar{Y} = |h|X + \bar{N} \tag{15}$$

where $\bar{N} \sim \mathcal{CN}(0, N_0)$. the effective signal is now $|h|X$, which can one of three (real) values $\{-|h|A, 0, |h|A\}$. Since the effective signal is real-valued, we need only the real part of $\bar{Y}$ for detection. Therefore, from (15), we have [15%]

$$\Re(\bar{Y}) = |h|X + \Re(\bar{N}) \tag{16}$$

where $\Re(\bar{N}) \sim \mathcal{N}(0, \frac{N_0}{2})$. This is identical to the detection problem in part (a), except that the symbols are now $\{-|h|A, 0, |h|A\}$. Therefore the error probability conditioned on h is

$$P_{e|h} = \frac{4}{3}\mathcal{Q}\left(\sqrt{\frac{(|h|A)^2}{2N_0}}\right) = \frac{4}{3}\mathcal{Q}\left(\sqrt{\frac{3|h|^2E_s}{4N_0}}\right).$$

ii) Using the Q-approximation,

$$P_{e|h} \approx \frac{2}{3}e^{\frac{-3|h|^2E_s}{8N_0}}.$$

The probability of error averaged over all realisations of h is [15%]

$$P_e = \int_0^\infty \frac{2}{3}e^{\frac{-3E_s}{8N_0}x}e^{-x}\,dx = \frac{2}{3}\left(\frac{1}{1+\frac{3E_s}{8N_0}}\right).$$

iii) Let $snr = E_s/N_0$. Then from part (a),

$$P_{e,AWGN} = \frac{4}{3}\mathcal{Q}\left(\sqrt{\frac{3snr}{4}}\right) \approx \frac{2}{3}e^{-\frac{3snr}{8}}$$

which decreases *exponentially* with growing snr. On the other hand [20%]

$$P_{e,fading} = \frac{2}{3}\left(\frac{1}{1+3snr/8}\right)$$

which decreases as $1/snr$, i.e., much more slowly as snr increases.

We can use diversity to improve the probability of error in a fading channel. If we transmit information through L independently faded signal paths, the probability of error will decay as $\sim snr^{-L}$. One way to achieve this is through time diversity, where the symbols of a codeword are interleaved with the symbols of other codewords, so that each symbols of a codeword experiences independent fading.