Dr R Venkataramanan

4F5 Advanced Communications and Coding Engineering Tripos 2015/16 – Solutions

Question 1

(a) i) Denote the pmf of Z as $p_z(r)$ for $r \in \{2, 3, \dots, 8\}$:

$$p_Z(r) = \sum_{k=1}^{2} p(k)p(r-k).$$

Using this, we find [15%]

$$p_z(2) = p(1)p(1) = \frac{1}{16},\ p_z(3) = 2p(1)p(2) = \frac{2}{16},\ p_z(4) = 2p(1)p(3) + p(2)p(2) = \frac{3}{16},$$
$$p_z(5) = \frac{4}{16},\quad p_z(6) = \frac{3}{16},\quad p_z(7) = \frac{2}{16},\quad p_z(8) = \frac{1}{16}.$$

ii) The entropy $H(Z) = \sum_{r=2}^{8} p_z(r) \log_2 \frac{1}{p_z(r)}$. Using the above pmf, we find this to be

$$H(Z) = 2.656 \text{ bits.}$$

The entropy $H(X) = \sum r = 1^4 \frac{1}{4} \log_2 4 = 2$ bits. [15%]

iii) From the chain rule, we have

$$H(Y,Z) = H(Z) + H(Y|Z). \tag{1}$$

We can also write

$$H(Y,Z) = H(Y) + H(Z|Y) = H(Y) + H(X|Y) = H(Y) + H(X). \tag{2}$$

The last two equalities hold because $H(Z|Y) = H(X+Y|Y) = H(X|Y)$, which equals $H(X)$ since X and Y are independent. From (1) and (2), we conclude that [20%]

$$H(Y|Z) = H(Y) + H(X) - H(Z) = 2 + 2 - 2.656 = 1.344 \text{ bits.}$$

iv) The typical set for Z^n, denoted by $A_{\epsilon,n}(Z)$, will consist of sequences that each contain approximately 6.25% 2's, 12.5% 3's, 18, 75% 4's, 25% 5's, 18.75% 6's, 12.5% 7's, and 6.25% 8's. The number of sequences in $A_{\epsilon,n}(X)$ will be close to $2^{nH(Z)} = 2^{2.656n}$. [10%]

(b) i) Using the chain rule on the LHS, we get

$$H(X,Y,Z) - H(X,Y) = H(X,Y) + H(Z|X,Y) - H(X,Y) = H(Z|X,Y). \tag{3}$$

On the RHS we get,

$$H(X,Z) - H(X) = H(X) + H(Z|X) - H(X) = H(Z|X). \tag{4}$$

Since conditioning can only decrease entropy, we have $H(Z|X,Y) \leq H(Z|X)$. Thus (3) and (4) imply the required inequality. For equality, we need $H(Z|X,Y) \leq H(Z|X)$, which occurs when $P_{Z|X,Y} = P_{Z|X}$, i.e., $Z - X - Y$ form a Markov chain. [15%]

ii) Using the chain rule on the LHS, we get

$$\begin{aligned} H(X,Z \mid Y) + H(Y) - H(Z) &= H(X|Z,Y) + H(Z|Y) + H(Y) - H(Z) \\ &= H(X|Z,Y) + H(Z,Y) - H(Z) \\ &= H(X|Z,Y) + H(Z) + H(Y|Z) - H(Z) \\ &= H(X|Z,Y) + H(Y|Z) \\ &\leq H(X|Z) + H(Y|Z). \end{aligned} \tag{5}$$

where the last inequality holds because conditioning cannot decrease entropy. For equality to hold, we need $H(X|Z,Y) = H(X|Z)$, i.e., $P(X|Z,Y) = P(X|Z)$, i.e., $X - Z - Y$ form a Markov chain. [25%]

Assessor's Comment: *Part (a) was straightforward answered well, though many students did not describe the typical set properly, especially the size. Many good attempts on part (b), but very few gave the correct conditions for equality to hold in the given information inequalities.*

Question 2

(a) i) The transition matrix is:

		$\underline{Y}$			
	$P(\underline{Y}\mid\underline{X})$	0ϵ	$\epsilon 0$	1ϵ	$\epsilon 1$
$\underline{X}$	00	$\frac{1}{2}$	$\frac{1}{2}$	0	0
	10	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	01	$\frac{1}{2}$	0	0	$\frac{1}{2}$
	11	0	0	$\frac{1}{2}$	$\frac{1}{2}$

[10%]

ii) The mutual information for the channel is

$$I(\underline{X};\underline{Y}) = H(\underline{Y}) - H(\underline{Y}|\underline{X}) = H(\underline{Y}) - \sum_{\underline{x}} P(\underline{x}) H(Y|X = \underline{x}). \tag{6}$$

Next, note that given any two-bit $\underline{x}$, there are two equally likely choices for $\underline{Y}$, hence

$$H(\underline{Y}|X = \underline{x}) = 1 \quad \forall \underline{x}.$$

Therefore,

$$I(\underline{X};\underline{Y}) = H(\underline{Y}) - 1 \leq \log_2 4 - 1 = 1 \text{ bit}. \tag{7}$$

The inequality holds because $\underline{Y}$ takes one of four values, hence $H(\underline{Y}) \leq \log_2 4 = 2$ bits.

Assigning equal probability 1/4 to all four input bit-pairs, yields $P(\underline{Y} = 0\epsilon) = P(\underline{Y} = \epsilon 0) = P(\underline{Y} = 1\epsilon) = P(\underline{Y} = \epsilon 1) = \frac{1}{4}$. (This can be checked using values in the transition matrix above.) This choice gives $H(\underline{Y}) = 2$ bits, which is the maximum possible value.

Therefore the capacity is $\max_{P(\underline{X})} I(\underline{X};\underline{Y}) = 1$ bit/channel use. [25%]

iii) We can transmit 1 bit of information per channel use by choosing two non-confusable inputs, e.g, $\underline{X} \in \{00, 11\}$, using one of these to signal a 0, and the other to signal a 1. (We could also use $\{01, 01\}$ as the non-confusable two inputs.) Note that this input distribution is different from the one used for the capacity computation in (ii) above. With a uniform input distribution as in (ii), the capacity-achieving coding scheme would be much more complicated (long codewords constructed with random coding, joint typicality/ML decoding etc.) [15%]

(b) (i) The rate is the number of source digits divided by the number of code digits, [10%]

$$R = \frac{d^2}{(d+1)^2}$$

(ii) The factor graph has 9 variable nodes and 6 constraint nodes. Each variable node is involved in 2 constraints and hence has degree 2. Each constraint node involves 3 variables and hence has degree 3. This is a regular $(d_v, d_c) = (2, 3)$ code. [15%]

(iii) The design rate for this regular low-density parity-check (LDPC) code is

$$R_d = 1 - \frac{d_v}{d_c} = 1 - \frac{2}{3} = \frac{1}{3}.$$

This differs from the true rate of $R = d^2/(d+1)^2 = 4/9$ obtained previously. The reason for this discrepancy is that one of the constraints in the parity-check matrix implied by the factor graph is redundant. The factor graph implies a 6×9 parity-check matrix but the code dimensions imply a $(9-4) \times 9 = 5 \times 9$ parity-check matrix. [25%]

Assessor's Comment: *The channel transition matrix and capacity computation in part (a) was answered well by almost all who attempted this question. Part (b) was answered less well. Most students did not correctly specify the number of variable/constraint nodes and their degrees.*

Question 3

(a) The parity-check matrix consists of the first two rows of the DFT matrix [10%]

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \end{bmatrix}.$$

(b) A Reed Solomon code is Maximum Distance Separable (MDS), i.e., $N - K + 1 = d_{\min}$. This code has code length $N = 5$, encodes $K = 3$ key digits, and hence $d_{\min} = 5 - 3 + 1 = 3$. [10%]

(c) The key has $5 - 2 = 3$ digits over GF(11) so there are $11^3 = 1331$ possible key combinations. Only one of those is correct so the probability of selecting it when the key is chosen uniformly at random is $1/1331 = .00075$ [10%]

(d) A Reed Solomon decoder can recover from any pattern of t errors where t is the largest number such that $2t < d_{\min}$. In our case, $d_{\min} = 3$, $t = 1$, so a single error can be corrected, allowing the four directors to recover the correct digit of the fifth director if their initial assumption is wrong. [10%]

(e) Multiplying the assumed sequence of digits by the parity-check matrix, we obtain

$$[6, 5, 5, 5, 0] \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \end{bmatrix}^T = [10, 8].$$

Since the result is not $[0, 0]$, we conclude that the assumed sequence is not a codeword and hence the assumption that the fifth digit is zero is wrong. [15%]

(f) We take the DFT of the sequence $6, 5, 5, 5, 0$ to obtain

$$[6, 5, 5, 5, 0] \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \\ 1 & 5 & 3 & 4 & 9 \\ 1 & 9 & 4 & 3 & 5 \\ 1 & 3 & 9 & 5 & 4 \end{bmatrix} = [10, 8, 0, 9, 3].$$

We look for the recurrence relation of order 1 that generates the first two digits $[10, 8]$ and find

$$x_2 = 3x_1$$

since $3 \cdot 10 = 30 \mod 11 = 8$. Hence we reconsitute the Fourier domain error sequence

$$[10, 8, 2, 6, 7]$$

and substract it from $[10, 8, 0, 9, 3]$ to yield

$$[10, 8, 0, 9, 3] - [10, 8, 2, 6, 7] = [0, 0, 9, 3, 7]$$

hence the secret key is $[9, 3, 7]$. [30%]

Alternate Solution: Setting the missing digit to x, for the parity check equations to be satisfied we need

$$[6, 5, 5, 5, x] \begin{bmatrix} 1 & 1 \\ 1 & 4 \\ 1 & 5 \\ 1 & 9 \\ 1 & 3 \end{bmatrix} = [0, 0].$$

Solving either of the two equations gives $x = 1$. Take DFT of the codeword $[6, 5, 5, 5, 1]$ to recover the secret key.

(g) The Reed Solomon code can recover codewords with $d_{\min} - 1 = 2$ erasures. Hence if any 2 directors are missing (erased), the three remaining directors should in theory be able to recover the key to unlock the database.

The alternate solution to part (f) suggests how one could recover two erased code digits: set the erased digits to x, y and recover them from the two parity check equations.

[15%]

Assessor's Comment: *For part (f), a lot of students took a long route to getting the secrete by computing the IDFT to recover the error sequence, then recovering the codeword etc. As described above, an easier way is to recover the secrete key directly by subtracting the Fourier domain error sequence from the DFT of the given length 5 sequence. There were a few clever solutions which set the missing code digit to x, solved the resulting parity check equation to recover x, and then took the DFT to get the secret key.*

Question 4

(a) i) The detector first multiplies Y by $h^*/|h|$ to obtain the modified output

$$\bar{Y} = |h|x + \bar{N} \tag{8}$$

The noise $\bar{N}$ is a complex Gaussian rv $\sim \mathcal{CN}(0, N_0)$. The input symbol to this modified channel (8) is $|h|x$ where x is a symbol from the QPSK constellation. Scaling each constellation symbol by the real number $|h|$ does not change the optimal decision regions. Therefore, [15%]

$$\hat{X} = \begin{cases} (A, A) & \text{if } \bar{Y}_R \geq 0, \bar{Y}_I \geq 0 \\ (A, -A) & \text{if } \bar{Y}_R \geq 0, \bar{Y}_I < 0 \\ (-A, -A) & \text{if } \bar{Y}_R < 0, \bar{Y}_I < 0 \\ (-A, A) & \text{if } \bar{Y}_R < 0, \bar{Y}_I \geq 0 \end{cases}$$

where we have denoted the real and imaginary parts of $\bar{Y}$ by $\bar{Y}_R$ and $\bar{Y}_I$.

ii) Due to symmetry of the constellation,

$$P_{e|h} = P(\hat{X} \neq p_i \mid X = (A, A))$$

By symmetry, $P(\hat{X} \neq p_i \mid X = p_i)$ is the same for $i = 1, \ldots, 4$. Therefore

$$\begin{aligned} P_e &= P(\bar{Y}_R < 0 \ \cup \ \bar{Y}_I < 0 \mid X = (A, A)) \\ &= P\left(|h|A + N_R < 0 \ \cup \ |h|A + N_I < 0 \mid X = (A, A)\right) \\ &= P\left(\{N_R < -|h|A\} \ \cup \ \{N_I < -|h|A\}\right) \leq P(N_R < -|h|A) + P(N_I < -|h|A) = 2\mathcal{Q}\left(\frac{|h|A}{\sqrt{N_0/2}}\right). \end{aligned}$$

The energy per symbol $E_s = 2A^2$. Also $E_s = E_b \log 4 = 2E_b$. Therefore, $A^2 = E_b$, or $A = \sqrt{E_b}$. [20%]
Using this in (a), we conclude that $P_{e|h} \leq 2\mathcal{Q}\left(\sqrt{\frac{2|h|^2 E_b}{N_0}}\right)$.

iii) Using the bound $\mathcal{Q}(x) < \frac{1}{2}e^{-x^2/2}$ for $x > 0$, the prob. of error given h can be bounded as

$$P_{e|h} \leq 2\mathcal{Q}\left(\sqrt{\frac{2|h|^2 E_b}{N_0}}\right) < \exp\left(-\frac{|h|^2 E_b}{N_0}\right).$$

Using $f_{|h|^2}(x) = e^{-x}, \ x \geq 0$, the probability of error averaged over all realisations of h is [10%]

$$P_e = \mathbb{E}[P_{e|h}] \leq \mathbb{E}\left[e^{-\frac{E_b}{N_0}|h|^2}\right] = \int_0^\infty e^{-\frac{E_b}{N_0}x} e^{-x}\, dx = \left(1 + \frac{E_b}{N_0}\right)^{-1}. \tag{9}$$

(b) i) Conjugating the second output $Y[2]$, the vector at the output of the demodulator becomes

$$\begin{aligned} Y[1] &= \ \ u h_a + v h_b + N[1] \\ Y^*[2] &= -u h_b^* + v h_a^* + N[2] \end{aligned}$$

Let $\mathbf{h} = [h_a, h_b]$ and $\|\mathbf{h}\| = \sqrt{|h_a|^2 + |h_b|^2}$.

1) Take inner product of the vector $[Y[1], Y[2]^*]$ with the vector $\frac{1}{\|\mathbf{h}\|}[h_a^*, -h_b]$ to get:

$$\bar{Y} = \|\mathbf{h}\| u + \bar{N} \tag{10}$$

2) Take inner product of the vector $[Y[1], Y[2]^*]$ with the vector $\frac{1}{\|\mathbf{h}\|}[h_b^*, h_a]$ to get:

$$\bar{Y}' = \|\mathbf{h}\| v + \bar{N}' \tag{11}$$

The noise rvs $\bar{N}$ and $\bar{N}'$ are each $\mathcal{CN}(0, N_0)$. Can now detect u from $\bar{Y}$ and v from $\bar{Y}'$ *separately.* Since u, v are each drawn from the above QPSK constellation, the decision regions for each detector are the same as in (a).(i). [20%]

ii) Using the calculation in (a).(ii), the probability of detection error for each of the QPSK symbols u, v is $2\mathcal{Q}\left(\sqrt{\frac{2\|\mathbf{h}\|^2 E_b}{N_0}}\right)$. The probability of detection error for the pair (u, v) is the probability that at least one of them is detected wrongly, and can be bounded as

$$P_{e|\mathbf{h}} \leq 4\mathcal{Q}\left(\sqrt{\frac{2\|\mathbf{h}\|^2 E_b}{N_0}}\right) < 2\exp\left(-\frac{\|\mathbf{h}\|^2 E_b}{N_0}\right),$$

where the last inequality is obtained using $\mathcal{Q}(x) < \frac{1}{2}e^{-x^2/2}$ for $x > 0$. The probability of error averaged over all realisations of $\mathbf{h}$ is [20%]

$$\begin{aligned} P_e = \mathbb{E}[P_{e|\mathbf{h}}] &\leq \mathbb{E}\left[2\exp\left(-\frac{\|\mathbf{h}\|^2 E_b}{N_0}\right)\right] \\ &= 2\mathbb{E}\left[e^{-\frac{E_b}{N_0}|h_a|^2} e^{-\frac{E_b}{N_0}|h_b|^2}\right] = 2\left(\int_0^\infty e^{-\frac{E_b}{N_0}x} e^{-x}\, dx\right)^2 = 2\left(1 + \frac{E_b}{N_0}\right)^{-2}. \end{aligned} \tag{12}$$

iii) The schemes in parts (a) and (b) both have the same rate of 1 QPSK symbol/time-period (2 bits/time period). As the snr E_b/N_0 increases, comparing (12) and (9), we see that the 2-Tx antenna scheme has a much faster decay of error probability. This is due to the diversity gain of 2 provided by the two transmit antennas. However, since each antenna is transmitting a QPSK symbol in each time-period, the 2-Tx antenna scheme has twice the transmit power of the single antenna scheme in part (a). [15%]

Assessor's Comment: *Part (a) was well answered, though made mistakes in computing the average energy per bit. In part (b), many students forgot to normalise while multiplying the outputs by the fading coefficients. Many also failed to point out that the transmission scheme with two antennas has double the transmission power.*