Version AGiF/2

EGT3
ENGINEERING TRIPOS PART IIB

Thursday 5 May 2022 9.30 to 11.10

Module 4F5

ADVANCED INFORMATION THEORY & CODING

*Answer not more than **three** questions.*

All questions carry the same number of marks.

*The **approximate** percentage of marks allocated to each part of a question is indicated in the right margin.*

*Write your candidate number **not** your name on the cover sheet.*

STATIONERY REQUIREMENTS
Single-sided script paper

SPECIAL REQUIREMENTS TO BE SUPPLIED FOR THIS EXAM
CUED approved calculator allowed
Engineering Data Book

10 minutes reading time is allowed for this paper at the start of the exam.

You may not start to read the questions printed on the subsequent pages of this question paper until instructed to do so.

You may not remove any stationery from the Examination Room.

1 (a) Rabbi Levi ben Gershon proved in 1343 that there are no solutions to the equation

$$3^m + 1 = 2^n$$

other than $(m, n) = (0, 1)$ and $(m, n) = (1, 2)$. Prove this theorem by taking the remainder of both sides of the equation when divided by 8. [10%]

(b) Does 28 have a multiplicative inverse in arithmetic modulo 385? Justify your answer. [10%]

(c) What is the companion matrix of X in GF(32) defined via the primitive polynomial $\pi(X) = 1 + X^2 + X^5$? [10%]

(d) What is the multiplicative order of $1 + X + X^2 + X^4$ in GF(32)? [10%]

(e) What is the dimension of the code generated by the matrix

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

over GF(4), how many codewords does it contain, and what is its minimum distance $d_{\min}$? [10%]

(f) In a toy example of the Rivest-Shamir-Adelmann (RSA) cryptosystem using small primes, your public key is $(247, 97)$ where only you know the prime factorisation of $247 = 13 \times 19$. Juliet's public key is $(187, 7)$ and Romeo's public key is $(391, 5)$. You receive a signed cryptogram $(y_1, y_2) = (175, 10)$ where y_1 is a secret message encrypted using your public key, and y_2 is the cryptogram y_1 re-encrypted using your correspondent's secret key to serve as signature.

(i) Decrypt the cryptogram y_1 and recover the secret message. [40%]

(ii) Determine who the message is from by verifying your correspondent's signature. [10%]

2 (a) What are the possible lengths of a Reed-Solomon code defined over GF(29)? [10%]

(b) A Reed-Solmon code is defined using $\alpha = 12$. What is its code length? [10%]

(c) Write out the Discrete Fourier Transform (DFT) matrix that this code is based on. [10%]

(d) An information sequence of length 2 is mapped to a codeword by prepending the information sequence with two zeros and multiplying the resulting vector by the inverse DFT matrix. What is the code's parity-check matrix? [10%]

(e) What is the code's encoder matrix? It may be helpful to note that $R_{29}(4 \times 22) = 1$. [10%]

(f) A codeword is transmitted over a channel that makes at most one error over the length of a codeword, and the received word is $\mathbf{r} = [3, 11, 11, 3]$ whose DFT is $\mathbf{R} = [28, 1, 0, 12]$. What were the encoded information digits? [20%]

(g) A codeword is transmitted over an erasure channel and the received word is $\mathbf{r} = [?, ?, 5, 21]$. If we replace the erasures by 0s, what is the recurrence relation that generates the error sequence in the frequency domain? [20%]

(h) Given that the DFT of $[0, 0, 5, 21]$ is $[26, 4, 13, 15]$, what were the encoded information digits in the transmission over the erasure channel? [10%]

3 Let $P_{Y|X}(y|x)$ be the transition probability assignment of a discrete memoryless channel and let $P_V(v)$ be the probability distribution of a discrete memoryless source. For $0 \leq \rho \leq 1$, consider the functions

$$E_s(\rho) = \log \left(\sum_{v \in \mathcal{V}} P_V(v)^{\frac{1}{1+\rho}} \right)^{1+\rho}$$

$$E_0(\rho, P_X) = -\log \sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} P_X(x) P_{Y|X}(y|x)^{\frac{1}{1+\rho}} \right)^{1+\rho}.$$

(a) Sketch the function $E_s(\rho)$ and explain how it can be used to show that there exist fixed-length source codes of rate $R = \frac{1}{n} \log_2 M$ such that for $R > H(V)$, the average probability of error $\bar{p}_e \to 0$ as $n \to \infty$, where M is the number of indices that are used for compression. [20%]

(b) Sketch the function $E_0(\rho, P_X)$ and explain how it can be used to show that there exist channel codes of rate $R = \frac{1}{n} \log_2 M$ such that for $R < I(X;Y)$, the average probability of error $\bar{p}_e \to 0$ as $n \to \infty$, where M is the number of codewords. [20%]

(c) Consider a separate source-channel coding scheme in which a fixed-length source coding system of a discrete memoryless source $P_V(v)$ maps source sequences v^n onto messages $m \in \{1, \ldots, M\}$. The output of the source encoder is fed to a channel encoder that maps each message m onto a codeword x_m^n for $m \in \{1, \ldots, M\}$ and sends x_m^n over discrete memoryless channel $P_{Y|X}(y|x)$. At the decoder, the channel decoder estimates the message $\hat{m} \in \{1, \ldots, M\}$ upon observing the received sequence y^n. Upon observing $\hat{m}$, the source decoder estimates the source sequence $\hat{v}^n$.

(i) Sketch the end-to-end block diagram of the system, appropriately labelling each of the variables. [10%]

(ii) Show that the error probability of this system $p_e \triangleq \mathbb{P}[\hat{V}^n \neq V^n]$ can be bounded as

$$p_e \leq \mathbb{P}[\hat{V}^n \neq V^n | \hat{m} = m] + \mathbb{P}[\hat{m} \neq m]. \quad [20\%]$$

(iii) For random fixed-length source coding with maximum metric decoding and random channel coding with maximum-likelihood decoding, show that

$$\bar{p}_e \leq e^{-n(\rho_s R - E_s(\rho_s))} + e^{-n(E_0(\rho_c, P_X) - \rho_c R)}$$

for $\rho_s, \rho_c \in [0, 1]$. [15%]

(iv) How should R be chosen as a function of $H(V), I(X;Y)$ so $\bar{p}_e \to 0$ for $n \to \infty$? [15%]

4 (a) Consider a code $\mathcal{C}_n$ of length n with M codewords and denote by C_n the random set whose realisations are randomly generated codes $\mathcal{C}_n$. Denote the error probability of a randomly generated code by $p_e(\mathcal{C}_n)$, and its expectation by $\mathbb{E}[p_e(\mathsf{C}_n)]$.

(i) Show that for any $s > 0$ and positive real-valued sequence γ_n it holds that

$$\mathbb{P}\left[p_e(\mathcal{C}_n) \geq \gamma_n^{\frac{1}{s}}\, \mathbb{E}[p_e(\mathsf{C}_n)^s]^{\frac{1}{s}}\right] \leq \frac{1}{\gamma_n}. \qquad [15\%]$$

(ii) Show that with probability higher than $1 - \frac{1}{\gamma_n}$ we have that

$$p_e(\mathcal{C}_n) < \gamma_n^{\frac{1}{s}}\, \mathbb{E}[p_e(\mathsf{C}_n)^s]^{\frac{1}{s}}. \qquad [10\%]$$

(iii) What conditions does the real-valued sequence γ_n need to fulfill so that when $n \to \infty$ with probability approaching one the following holds

$$-\frac{1}{n}\log p_e(\mathcal{C}_n) > -\frac{1}{n}\log \mathbb{E}[p_e(\mathsf{C}_n)^s]^{\frac{1}{s}}. \qquad (1)$$

[15%]

(iv) Explain the meaning of the result in Eq. (1) for $s = 1$. [10%]

(b) Suppose we are given i.i.d. observations $y^n = (y_1, \ldots, y_n)$. We wish to decide whether they have been generated from distributions P^n or Q^n.

(i) Explain what the Stein exponent is and what it means in the context of hypothesis testing. [15%]

(ii) Find the Stein exponent for distributions

$$P(y) = 2^{-y}, \quad Q(y) = q \cdot p^{y-1}$$

defined for $y = 1, 2, 3, \ldots$. Hint: use the fact that $\mathbb{E}_P[Y] = 2$, where $\mathbb{E}_P[Y]$ denotes the expectation of Y with respect to distribution P. [20%]

(iii) Assume the observations are such that $y_i \in \mathcal{A}$, where $\mathcal{A} = \{1, 2, \ldots, A\}$, for $i = 1, \ldots, A$. Assume the distributions are

$$P(y) = \alpha\, e^{-y}, \quad Q(y) = \frac{1}{A}.$$

Show that the Stein exponent is equal to

$$\log \alpha + \log A - \mathbb{E}_P[Y]$$

where $\mathbb{E}_P[\cdot]$ denotes expectation with respect to distribution P. [15%]

END OF PAPER

THIS PAGE IS BLANK