Version AGiF/2

EGT3
ENGINEERING TRIPOS PART IIB

Monday 12 May 2025 2 to 3.40

Module 4F5

ADVANCED INFORMATION THEORY AND 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) Below are the steps of a proof that 19 divides $3 + 2^{2^{6k+2}}$ for all integers k, but we have omitted the justification for each step. Explain why each step holds, and how they link together to prove the statement. [25%]

(i) $R_9(2^{6k}) = 1$

(ii) $R_{18}(2^{6k+2}) = R_9(2^{6k+2}) = 4$

(iii) $R_{19}(2^{18}) = 1$

(iv) $R_{19}(2^{2^{6k+2}}) = R_{19}(2^{18q+4}) = R_{19}(2^4) = 16$

(b) We define arithmetic in GF(32) with irreducible polynomial $\pi(X) = 1 + X^2 + X^5$. [25%]

(i) What is $(1 + X + X^3) + (X + X^2 + X^3)$?

(ii) What is $(1 + X + X^3)(X + X^2 + X^3)$?

(iii) What is the companion matrix of $(X + X^2 + X^3)$?

(iv) Is $\pi(X)$ a primitive polynomial?

(v) What is the multiplicative order of the element $1 + X$?

(c) Having limited access to a large prime number generator for the RSA cryptosystem, an apprentice cryptographer Bob implements RSA using only one large prime p instead of two primes p_1 and p_2. In RSA, a user's public key is (m, e) where $m = p_1 p_2$. In Bob's implementation, $m = p^2$. Help Bob by answering the following questions:

(i) Bob knows that for standard RSA, a secret key d is generated using the Extended Euclid Algorithm such that $R_w(d \times e) = 1$ where $w = (p_1 - 1)(p_2 - 1)$. By analogy, Bob tried to find a key d such that $R_w(d \times e) = 1$ where $w = (p - 1)^2$ but this did not work: when he tried to encrypt a secret message x, he found that $R_{p^2}(x^{de}) \neq x$. What should Bob change to make it work? [10%]

(ii) Assuming that you have fixed this issue so that $R_{p^2}(x^{de}) = x$ for most x, explain what would happen if one tried to encrypt and decrypt a message $x = qp$ for some number q, and comment on whether this is a significant weakness. [10%]

(iii) Play out a toy example of Bob's cryptosystem using $p = 11$ and $e = 3$. What is the public key? Compute d. Encrypt the message $x = 10$ and decrypt the result. [20%]

(iv) Alice, a far more experienced cryptographer, hears of Bob's creative meddling with RSA and sends him an urgent telegram to warn him that his system is not secure, assuming that it will be used in accordance with Kerckhoff's principle, despite the fact that it encrypts and decrypts correctly. Can you think why this is the case? [10%]

2 (a) Reed-Solomon (RS) codes are MDS, i.e., they satisfy Singleton's bound with equality. Nevertheless, when used for error correction, there are certain sets of parameters that result in a sub-optimal code whose rate can be increased without sacrificing error correction performance. For example, explain how a Reed-Solomon code defined over GF(256) with information length $K = 242$ and code length $N = 255$ can be improved in such a way, and comment on whether the same argument applies when Reed Solomon codes are used for erasure recovery. [15%]

(b) What are the possible code lengths for a Reed-Solomon code over GF(31)? [10%]

(c) Specify the Discrete Fourier Transform matrix over GF(31) with $W_N = \alpha = 4$ and determine the RS code length N. [15%]

(d) An information sequence of length 3 is mapped onto a codeword by prepending the information sequence with two zeros and multiplying the resulting vector by the inverse DFT matrix. What is the rate of this code and what is its parity-check matrix? [10%]

(e) Elements of GF(31) are mapped to characters using the conversion table in Fig. 1. The code is used to encode a 3 letter word. The codeword is transmitted with at most one error and received as **BFH=Z**. Recover the encoded word. [20%]

(f) Another codeword is transmitted over an erasure channel and received as **I=A##** where we used the symbol "**#**" to denote an erasure. Recover the encoded word. [30%]

Character	Element of GF(31)
=	0
A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26
+	27
-	28
*	29
/	30

Fig. 1

3 (a) Consider a source V^n over alphabet $\mathcal{V}$ with distribution P_{V^n}. Consider a block source code that assigns to each of the M most probable source sequences a unique codeword (assume $M < |\mathcal{V}|^n$); the remaining $|\mathcal{V}|^n - M$ source messages are all assigned the same codeword.

(i) Write an expression of the probability of error. [10%]

(ii) Explain why this is the code with minimum probability of error. [10%]

(iii) Hence, show that there exists a block source code for which

$$p_e \leq \mathbb{P}\left[\frac{1}{n}\log\frac{1}{P_{V^n}(V^n)} > \frac{1}{n}\log M\right]$$

[15%]

(iv) Show that for discrete memoryless sources, we can compress reliably for rates $R > H(V)$. [15%]

(b) Consider a hypothesis testing problem between two i.i.d. distributions P_1^n, P_2^n defined over alphabet $\mathcal{Y}^n$. Let H denote the true hypothesis and $\hat{H}$ the output of the test and $\pi_{i|j} = \mathbb{P}[\hat{H} = i|H = j]$, with $i, j \in \{1, 2\}$.

(i) State Stein's lemma, explain the result and illustrate its significance. [20%]

(ii) Suppose we want to design a test such that $\pi_{1|2} \leq 0.001$ and $\pi_{2|1} \leq 10^{-40}$. What is the minimum required sample size n that will guarantee the design constraints? [20%]

(iii) What is the minimum required sample size n if now $\pi_{1|2} \leq 0.00001$ and $\pi_{2|1} \leq 10^{-40}$? [10%]

4 Consider a discrete memoryless channel defined by $W^n(y^n|x^n) = \prod_{i=1}^n W(y_i|x_i)$, where $W(y|x)$ the probability of $y \in \mathcal{Y}$ being the output when $x \in \mathcal{X}$ is the input, with $\mathcal{Y}, \mathcal{X}$ being the output and input alphabets, respectively. Let the code be $\mathcal{C} = \{x^n(1), \ldots, x^n(M)\}$ where $x^n(j) \in \mathcal{X}^n$. Consider a random decoder that for a given channel output $y^n \in \mathcal{Y}^n$ outputs decoded message $\hat{m} = j$ with probability

$$\mathbb{P}[\hat{m} = j | Y^n = y^n] = \frac{W^n(y^n|x^n(j))}{\sum_{m'=1}^M W^n(y^n|x^n(m'))} \tag{1}$$

for $j = 1, \ldots, M$. The purpose of this question is to show that this suboptimal random decoder also achieves capacity.

(a) Consider the transmission of message $m = 1$. Show that the probability of correct decoding averaged over the random coding ensemble of independent codewords with probability $Q(x^n)$ is

$$\bar{p}_c = 1 - \bar{p}_e = \sum_{x^n, y^n} Q(x^n) W^n(y^n|x^n) \mathbb{E}\left[\frac{W^n(y^n|x^n)}{W^n(y^n|x^n) + \sum_{m' \neq 1} W^n(y^n|X^n(m'))} \right]$$

where the expectation is over random codewords $X^n(2), \ldots, X^n(M)$. [10%]

(b) Show that

$$\bar{p}_c \geq \sum_{x^n, y^n} Q(x^n) W^n(y^n|x^n) \frac{1}{1 + \mathbb{E}\left[\sum_{m' \neq 1} \frac{W^n(y^n|X^n(m'))}{W^n(y^n|x^n)} \right]}$$

(Hint: Jensen's inequality states that for a convex function f and random variable X, $\mathbb{E}[f(X)] \geq f(\mathbb{E}[X])$). [15%]

(c) Show that

$$\bar{p}_c \geq \sum_{x^n, y^n} Q(x^n) W^n(y^n|x^n) \frac{1}{1 + (M-1)\mathbb{E}\left[\frac{W^n(y^n|\bar{X}^n)}{W^n(y^n|x^n)} \right]}$$

[15%]

(d) Using that $1 - \frac{1}{1+z} \leq \min\{1, z\}$ show that

$$\bar{p}_e \leq \sum_{x^n, y^n} Q(x^n) W^n(y^n|x^n) \min\left\{ 1, (M-1) \frac{\mathbb{E}[W^n(y^n|\bar{X}^n)]}{W^n(y^n|x^n)} \right\}$$

[15%]

(e) Hence show that for $Q(x^n) = \prod_{i=1}^{n} Q(x_i)$,

$$\bar{p}_e \leq e^{-n(\bar{E}_0(\rho)-\rho R)}$$

using that $\min\{1, x\} \leq x^\rho$, $\rho \in [0, 1]$ where

$$\bar{E}_0(\rho) = -\log \sum_{x,y} Q(x)W(y|x)\left(\frac{\sum_{\bar{x}} Q(\bar{x})W(y|\bar{x})}{W(y|x)}\right)^\rho$$

[25%]

(f) Assuming $\bar{E}_0(\rho)$ is a concave function of ρ, show that the decoder described by Eq. (1) achieves the channel capacity $C = \max_Q I(X;Y)$. Justify your answer. [20%]

END OF PAPER

THIS PAGE IS BLANK