Version JS/2

EGT3
ENGINEERING TRIPOS PART IIB

---

Friday 1 May 2026 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) (i) Determine the Greatest Common Divisor of 2897643258 and 99. [10%]

(ii) Use the Chinese Reminder Theorem to show that $R_{341}(2^{340}) = 1$. [10%]
*Hint:* $341 = 11 \times 31$.

(iii) Test whether $1 + X + X^4$ is an irreducible polynomial over GF(2). [10%]

(iv) Is the irreducible polynomial $\pi(X) = 1 + X + X^7$ primitive? Justify your answer. [10%]

(v) What is the companion matrix of $X^3$ in $GF(32)$ with $\pi(X) = 1 + X^2 + X^5$? [10%]

(b) In a toy example of the Diffie-Hellman public key distribution system, we operate in $\langle \mathbb{Z}_p, \odot \rangle$ where $p = 47$ is a prime for which $p - 1 = 2 \times 23$ has a "large" prime factor. The generator is $\alpha = 5$. Your secret key is $x_A = 21$ and you wish to generate a common secret key to communicate with Bob whose public key is $y_B = 12$, which he derived from his secret key $x_B$.

(i) What is your public key $y_A$? [15%]

(ii) Use the Diffie-Hellman protocol to generate a common key. [15%]

(c) In a stream cipher, each $q$-ary plaintext symbol $X_k$ is combined with a pseudo-random $q$-ary symbol $E_k$ using a group operation $\oplus$ to yield a cyphertext symbol $Y_k$, i.e., $Y_k = X_k \oplus E_k$ for each $k \geq 0$. The pseudo-random symbol is generated by a recursive mapping $E_k = f_{\mathbf{s}}(E_{k-1}, E_{k-2}, \ldots, E_{k-\ell})$ for some $\ell$ and function $f_{\mathbf{s}}()$ that depends on the secret key $\mathbf{s}$. For this exercise, consider using a stream cipher over the additive group of $GF(q)$, and a linear function

$$f_{\mathbf{s}}(E_{k-1}, E_{k-2}, \ldots, E_{k-\ell}) = a_1 E_{k-1} + a_2 E_{k-2} + \ldots + a_\ell E_{k-\ell}$$

where the secret key is the set of coefficients and the initial state of the sequence, i.e., $\mathbf{s} = (a_1, \ldots, a_\ell, E_{-1}, \ldots, E_{-\ell})$.
A cryptanalist Eve is able to spy a portion of plaintext $X_{k_0}, X_{k_0+1}, \ldots, X_{k_0+L-1}$ of length $L$, allowing her to mount a "known plaintext" attack based on the plaintext/cyphertext pair of length $L$.

(i) Explain how Eve could determine the unknown coefficients and hence decrypt the complete cyphertext, and how large $L$ needs to be for her to achieve this. [10%]

(ii) Assuming that the known plaintext is of length $L = q - 1$ and is long enough for the attack devised in the previous part to succeed, if Eve doesn't know the parameter $\ell$, describe a method that would allow her to measure $\ell$ from the plaintext/cyphertext pair. [10%]

2 (a) Specify any three values of $q$ for which there exists a Reed Solomon (RS) code of length 7 over GF($q$). [10%]

(b) What are the possible code lengths for an RS code over GF(61)? [10%]

(c) Specify the Discrete Fourier Transform matrix over GF(61) with $W_N = \alpha = 9$ and determine the RS code length $N$. [10%]

(d) An information sequence of length 3 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 rate of this code and what is its parity-check matrix? [10%]

(e) The resulting codeword is received with at most one error as $(24, 12, 60, 50, 40)$. Recover the encoded information sequence. [20%]

(f) Another codeword is transmitted over an erasure channel and received as $(50, ?, ?, 33, 11)$ where we used the symbol $''?''$ to denote an erasure. Recover the encoded information sequence. [20%]

(g) The encoder used in the previous parts placed the information symbols in the frequency domain. If we wanted the information symbols to be the first part of the codeword in the time domain, what encoder (generator) matrix would we have to use to encode 3 information symbols? [20%]

*Hint:* it may be helpful to note that $R_{61}(24 \times 28) = 1$.

3 (a) The random-coding error exponent for source coding is given by

$$e_r(R) = \max_{0 \le \rho \le 1} \rho R - E_s(\rho)$$

where

$$E_s(\rho) = \log \left( \sum_v P_V(v)^{\frac{1}{1+\rho}} \right)^{1+\rho}$$

where $P_V$ is the source distribution.

(i) Explain what is the random-coding error exponent for source coding $e_r(R)$. [10%]

(ii) Let $H$ denote the smallest rate such that $e_r(R) > 0$. Show that [15%]

$$H = \min_{0 \le \rho \le 1} \frac{E_s(\rho)}{\rho}$$

(b) The random-coding error exponent for channel coding is given by

$$E_r(R) = \max_{0 \le \rho \le 1} E_0(\rho) - \rho R$$

where

$$E_0(\rho) = -\log \sum_y \left( \sum_x Q(x) W(y|x)^{\frac{1}{1+\rho}} \right)^{1+\rho}$$

where $W$ is the channel transition probability and $Q$ is the channel input distribution.

(i) Explain what is the random-coding error exponent for channel coding $E_r(R)$. [10%]

(ii) Let $C$ denote the largest rate such that $E_r(R) > 0$. Show that [15%]

$$C = \max_{0 \le \rho \le 1} \frac{E_0(\rho)}{\rho}$$

(c) Consider the binary erasure channel (BEC) with erasure probability $\delta$, shown in Fig 1. The transmitter sends a bit. The receiver either receives it correctly, or outputs an erasure symbol ? with probability $\delta$.

(i) Find the function $E_0(\rho)$ for the BEC. Then explain why the equiprobable input distribution $Q = [1/2,\ 1/2]$ maximizes $E_0(\rho)$ for this channel. [10%]

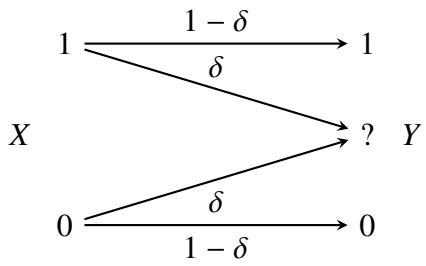


Fig. 1

(ii) It can be shown that $\frac{E_0(\rho)}{\rho}$ is non-increasing in $\rho$, so the maximum is achieved in the limit $\rho \to 0$. Use this fact to show that for the BEC with equiprobable input,

$$C = 1 - \delta$$

Hint: Let $f(r) = -\log\left(\delta + (1-\delta)2^{-r}\right)$. Then $\frac{df}{dr} = \frac{(1-\delta)2^{-r}}{\delta+(1-\delta)2^{-r}}$ [15%]

(iii) Now assume $\delta = 0$. Find and sketch $E_r(R)$ as a function of $R$. [10%]

(iv) If $\delta = 0$, it means that the erasure probability is exactly zero, which implies that the channel introduces no errors and the error exponent is infinite. However, from Part (c)(iii), you have observed that the random coding error exponent is finite for every $R \leq 1$. How do you explain and justify this observation? [15%]

4 Consider binary hypothesis testing between two i.i.d. distributions $P$ and $Q$ on a discrete alphabet $\mathcal{X}$.

(a) For a hypothesis test $T$, provide an expression for the type-I error $\varepsilon_0(P_{X^n}, T)$ and the type-II error $\varepsilon_1(Q_{X^n}, T)$. [10%]

(b) Explain the Neyman-Pearson setting and write its objective function. [10%]

(c) State Stein's lemma and the achievable exponents. [20%]

(d) While designing a hypothesis test, there may be situations where the test is not confident in its decision. One way to address this is to allow the test to output an erasure, denoted by e. Accordingly, we adjust the definitions of type-I and type-II errors so that erasures are not counted as errors. For $\delta > 0$, consider the following test

$$\phi_n(x^n) = \begin{cases} h_0 & \text{if } \frac{P_{X^n}(x^n)}{Q_{X^n}(x^n)} > e^{n[D(P\|Q)-\delta]} \\ h_1 & \text{if } \frac{Q_{X^n}(x^n)}{P_{X^n}(x^n)} > e^{n[D(Q\|P)-\delta]} \\ \text{e} & \text{otherwise} \end{cases} \tag{1}$$

(i) Show that

$$\lim_{n\to\infty} P_{X^n}\left[\phi_n(X^n) = \text{e}\right] = \lim_{n\to\infty} Q_{X^n}\left[\phi_n(X^n) = \text{e}\right] = 0$$

In other words, under this decision rule, the probability of an erasure can be made arbitrarily small, regardless of whether $P$ or $Q$ is the true distribution. (Hint: use the weak law of large numbers.) [20%]

(ii) For the type-I error, show that the test in Eq. (1) satisfies [20%]

$$P_{X^n}\left[\phi_n(X^n) = h_1\right] \le e^{-n[D(Q\|P)-\delta]}$$

(iii) It can be similarly shown that the test satisfies

$$Q_{X^n}\left[\phi_n(X^n) = h_0\right] \le e^{-n[D(P\|Q)-\delta]}$$

In other words, the test in Eq. (1) can attain the two Stein exponents simultaneously. Explain how this compares with classical binary hypothesis testing when the erasure option is not allowed. [20%]

**END OF PAPER**