Part II

Coding and Cryptography

Year

2023
2022
2021
2020
2019
2018
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005

Paper 1, Section I

3I Coding and Cryptography

(a) Let $\mathcal{A}$ be an alphabet of (finite) cardinality m. What does it mean to say that a code $c : \mathcal{A} \to \{0,1\}^*$ is (i) *prefix-free* or (ii) *optimal*?

Suppose that letters $\mu_1, \ldots, \mu_m$ are sent with probabilities $p_1, \ldots, p_m$. Let c be an optimal prefix-free binary code with word lengths $\ell_1, \ldots, \ell_m$.

Show that if $p_i > p_j$ then $\ell_i \leqslant \ell_j$. Show also that among the codewords of maximal length there must exist two that differ only in the last digit.

(b) Letters $\mu_1, \ldots, \mu_5$ are transmitted with probabilities $0.4, 0.2, 0.2, 0.1, 0.1$. Determine whether there are optimal binary codings with either (i) all but one codeword of the same length, or (ii) each codeword a different length. Justify your answers.

Paper 2, Section I

3I Coding and Cryptography

(a) (i) Consider a source $(X_n)_{n\geqslant 1}$ of random variables taking values in some finite alphabet $\mathcal{A}$. What does it mean for a source to be *Bernouilli*? What does it mean for a source to be *reliably encodable at rate* r? What is the *information rate* of a source?

(ii) Show that the information rate of a Bernouilli source $(X_n)_{n\geqslant 1}$ is at most the expected word length of an optimal code $c : \mathcal{A} \to \{0,1\}^*$ for X_1.

(b) Let $(X_n)_{n\geqslant 1}$ be a source with letters drawn from a finite alphabet $\mathcal{A}$. This source is not necessarily assumed to be Bernouilli. Let $N \geqslant 1$ be an integer and let $Y_i = (X_{(i-1)N+1}, X_{(i-1)N+2}, \ldots, X_{iN})$. Show that the information rate of the source $(Y_n)_{n\geqslant 1}$ is N times that for $(X_n)_{n\geqslant 1}$.

Paper 3, Section I

3I Coding and Cryptography

Let C be a binary linear $[n, m, d]$-code.

Define (i) the *parity check extension* C^+ of C and (ii) the *punctured code* C^- (assuming $n \geqslant 2$). Show that C^+ and C^- are both linear.

What is the *shortening* C' of C (assuming $n \geqslant 2$)? When is C' a linear code?

For the changes to C defined in (i) and (ii), describe the effect of both these changes on the generator and parity check matrices. For the case of (ii) you may assume that $d \geqslant 2$ and you puncture in the last place.

Paper 4, Section I

3I Coding and Cryptography

(a) If $C \subseteq \mathbb{F}_2^n$ is a linear code, define the *dual code* $C^\perp$ and explain why it is also linear. If C is cyclic, show directly that $C^\perp$ is cyclic. Explain briefly how the generator polynomials of C and $C^\perp$ are related.

(b) Factorise $X^7 - 1$ over the field $\mathbb{F}_2$ and hence list all the binary cyclic codes of length 7. Identify versions of Hamming's original code and its dual in your list. What are the other cyclic codes of length 7? You should relate them to codes defined explicitly in the course.

Paper 1, Section II

11I Coding and Cryptography

(a) What is a *binary symmetric channel* (BSC) with error probability p? Write down its channel matrix. Why can we assume that $p < \frac{1}{2}$? State Shannon's second coding theorem and use it to compute the capacity of this channel.

(b) Codewords 00 and 11 are sent with equal probability through a BSC with error probability p. Compute the mutual information between the codeword sent and the first digit received as output. Show that the extra mutual information gained on receipt of the second digit is $H(2p(1-p)) - H(p)$ bits. [Here $H(p)$ denotes the entropy of a random variable which takes the value 1 with probability p and 0 with probability $1-p$.]

(c) Consider a ternary alphabet and a channel that has channel matrix

$$\begin{pmatrix} 1-2\alpha & \alpha & \alpha \\ \alpha & 1-2\alpha & \alpha \\ \alpha & \alpha & 1-2\alpha \end{pmatrix}.$$

Calculate the capacity of the channel.

Paper 2, Section II

12I Coding and Cryptography

(a) What is a *one-time pad*?

Suppose that X and Y are independent random variables taking values in $\mathbb{Z}_n$, the integers modulo n. Using Gibbs' inequality, or otherwise, show that

$$H(X+Y) \geqslant \max\{H(X), H(Y)\}.$$

Why is this result of interest in the context of one-time pads? Does this result remain true if X and Y are not independent? Give reasons for your answer.

(b) The notorious spymaster Stan uses a one-time pad to communicate with the even more notorious spy Ollie. The messages are coded in the obvious way, namely, if the pad has C, the third letter of the alphabet and the message has I, the ninth, then the encrypted message has L as the $(3+9)$th. We will work modulo 26. Unknown to Stan and Ollie, the person whom they employ to carry the messages is actually the police agent Eve in disguise. The police are close to arresting Ollie when Eve is given the message

$$LRPFOJQLCUD.$$

Eve knows that the actual message is

$$FLYXATXONCE,$$

and wants to change things so that Ollie deciphers the message as

$$REMAINXHERE.$$

What message should Eve deliver?

(c) Let K be the field with 2^d elements. Recall that the multiplicative group $K^\times$ is a cyclic group; let α be a generator. Let $T : K \to \mathbb{F}_2$ be any non-zero $\mathbb{F}_2$-linear map. You are given that the $\mathbb{F}_2$-bilinear form $K \times K \to \mathbb{F}_2$ such that $(x, y) \mapsto T(xy)$ is non-degenerate (i.e. $T(xy) = 0$ for all $y \in K$ implies $x = 0$).

(i) Show that the sequence $x_n = T(\alpha^n)$ is the output from a linear feedback shift register of length at most d.

(ii) The *period* of $(x_n)_{n\geqslant 0}$ is the least integer $r \geqslant 1$ such that $x_{n+r} = x_n$ for all sufficiently large n. Show that the sequence in (i) has period $2^d - 1$.

Paper 1, Section I
3K Coding and Cryptography

(a) State *Kraft's inequality.*

Show that Kraft's inequality gives a necessary condition for the existence of a prefix-free code with given codeword lengths.

(b) A *comma code* is one where a special letter—the comma—occurs at the end of each codeword and nowhere else. Show that a comma code is prefix-free and give a direct argument to show that comma codes must satisfy Kraft's inequality.

Give an example of a non-decipherable code satisfying Kraft's inequality.

Paper 2, Section I
3K Coding and Cryptography

What is a *discrete memoryless channel* (DMC)? State *Shannon's second coding theorem.*

Consider two DMCs of capacities C_1 and C_2, each having input alphabet $\mathcal{A}$ and output alphabet $\mathcal{B}$. The *product* of these channels is a channel whose input and output alphabets are $\mathcal{A} \times \mathcal{A}$ and $\mathcal{B} \times \mathcal{B}$, respectively, with channel probabilities given by

$$\mathbb{P}(y_1 y_2 | x_1 x_2) = \mathbb{P}_1(y_1|x_1)\, \mathbb{P}_2(y_2|x_2),$$

where $\mathbb{P}_i(y|x)$ is the probability that y is received when x is transmitted through the ith channel $(i = 1, 2)$. Find the capacity of the product channel in terms of C_1 and C_2.

Paper 3, Section I
3K Coding and Cryptography

(a) Let C_1 and C_2 be (binary) linear codes with $C_2 \subseteq C_1$. Define their *bar product* $C_1|C_2$.

(b) (i) Let $d \geqslant 1$. Identify the Reed–Muller codes $\mathrm{RM}(d, 0)$ and $\mathrm{RM}(d, d)$ as well-known codes of a certain length. [Proofs are not required.]

For $0 < r < d$, identify the Reed–Muller code $\mathrm{RM}(d, r)$ as a bar product of certain Reed–Muller codes. [Proofs are not required.] Use this to compute the rank of $\mathrm{RM}(d, r)$.

(ii) By considering the original definition of Reed-Muller codes, show that every codeword in $\mathrm{RM}(d, d-1)$ has even weight. Deduce that $\mathrm{RM}(d, r)$ has dual code $\mathrm{RM}(d, d-r-1)$.

Paper 4, Section I
3K Coding and Cryptography

In this question we work over $\mathbb{F}_2$.

What is a *general feedback shift register of length* d with *initial fill* $(x_0, \ldots, x_{d-1})$? What does it mean for such a register to be *linear*?

Describe the Berlekamp–Massey method for breaking a cipher stream arising from a linear feedback shift register.

Use the Berlekamp–Massey method to find a linear recurrence with first eight terms $1, 1, 0, 0, 1, 0, 1, 1$.

Paper 1, Section II
11K Coding and Cryptography

(a) Let n be an odd integer. What does it mean to say that a code is a *cyclic code of length n with a defining set?* Define a *BCH code with design distance δ*. Show that a BCH code with design distance δ has minimum distance at least δ. [Properties of the Vandermonde determinant may be assumed.]

(b) Let $\alpha \in \mathbb{F}_{16}$ be a root of $X^4 + X + 1$. Let C be the BCH code of length 15 and design distance 5, with defining set the first few powers of α.

(i) Find the minimal polynomial for each element of the defining set, and hence find the generator polynomial of C.

(ii) Define the *error locator polynomial* $\sigma(X) \in \mathbb{F}_{16}[X]$ for any received word $r(X)$. [Properties of $\sigma(X)$ may be stated without proof.]

(iii) Suppose you receive the word $r(X) = 1 + X + X^7$. Find the error locator polynomial. Hence, either determine the error position or positions of $r(X)$, or explain why this is not possible.

Paper 2, Section II
12K Coding and Cryptography

(a) Consider two large distinct primes $p, q \equiv 3 \pmod 4$ and let $N = pq$. Briefly describe the *Rabin cipher* with modulus N.

I announce that I shall be using the Rabin cipher with modulus N. My friendly agent in Doxfor sends me a message m (with $1 \leqslant m \leqslant N-1$) encoded in the required form. Unfortunately, my cat eats the piece of paper on which the prime factors of N are recorded so I am unable to decipher it. I therefore find a new pair of primes and announce that I shall be using the Rabin code with modulus $N' > N$. My agent now re-encodes the message and sends it to me again.

The enemy agent Omicron intercepts both code messages. Show that Omicron can find m. Can Omicron decipher any other messages sent to me using only one of the coding schemes?

(b) Let p be a large prime and g a primitive root modulo p. What is the *discrete logarithm problem*? Explain what is meant by the *Diffie-Hellmann key exchange* and say briefly how an enemy can break the cipher if she can compute discrete logarithms efficiently.

Extend the Diffie–Hellman key exchange to cover three participants in a way that is likely to be as secure as the two-party system.

Extend the system further to n parties in such a way that they can compute their common secret key in at most $n^2 - n$ communications. (The numbers p and g of our original Diffie-Hellman system are known by everybody in advance.)

Paper 1, Section I

3K Coding and Cryptography

Let C be an $[n, m, d]$ code. Define the parameters n, m and d. In each of the following cases define the new code and give its parameters.

(i) C^+ is the parity extension of C.

(ii) C^- is the punctured code (assume $n \geqslant 2$).

(iii) $\overline{C}$ is the shortened code (assume $n \geqslant 2$).

Let $C = \{000, 100, 010, 001, 110, 101, 011, 111\}$. Suppose the parity extension of C is transmitted through a binary symmetric channel where p is the probability of a single-bit error in the channel. Calculate the probability that an error in the transmission of a single codeword is not noticed.

Paper 2, Section I

3K Coding and Cryptography

State Shannon's noisy coding theorem for a binary symmetric channel, defining the terms involved.

Suppose a channel matrix, with output alphabet of size n, is such that the entries in each row are the elements of the set $\{p_1, \ldots, p_n\}$ in some order. Further suppose that all columns are permutations of one another. Show that the channel's information capacity C is given by

$$C = \log n + \sum_{i=1}^{n} p_i \log p_i \,.$$

Show that the information capacity of the channel matrix

$$\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

is given by $C = \frac{5}{3} - \log 3$.

Paper 3, Section I

3K Coding and Cryptography

Let $d \geqslant 2$. Define the *Hamming code* C of length $2^d - 1$. Explain what it means to be a *perfect code* and show that C is a perfect code.

Suppose you are using the Hamming code of length $2^d - 1$ and you receive the message $111\ldots10$ of length $2^d - 1$. How would you decode this message using minimum distance decoding? Explain why this leads to correct decoding if at most one channel error has occurred.

Paper 4, Section I

3K Coding and Cryptography

Describe the Rabin scheme for coding a message x as x^2 modulo a certain integer N.

Describe the RSA encryption scheme with public key (N, e) and private key d.

[*In both cases you should explain how you encrypt and decrypt.*]

Give an advantage and a disadvantage that the Rabin scheme has over the RSA scheme.

Paper 1, Section II

11K Coding and Cryptography

Let $\Sigma_1 = \{\mu_1, \ldots, \mu_N\}$ be a finite alphabet and X a random variable that takes each value μ_i with probability p_i. Define the *entropy* $H(X)$ of X.

Suppose $\Sigma_2 = \{0, 1\}$ and $c : \Sigma_1 \to \Sigma_2^*$ is a decipherable code. Write down an expression for the expected word length $E(S)$ of c.

Prove that the minimum expected word length S^* of a decipherable code $c : \Sigma_1 \to \Sigma_2^*$ satisfies

$$H(X) \leqslant S^* < H(X) + 1\,.$$

[You can use Kraft's and Gibbs' inequalities as long as they are clearly stated.]

Suppose a decipherable binary code has word lengths $s_1, \ldots, s_N$. Show that

$$N \log N \leqslant s_1 + \cdots + s_N\,.$$

Suppose X is a source that emits N sourcewords $a_1, \ldots, a_N$ and p_i is the probability that a_i is emitted, where $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_N$. Let $b_1 = 0$ and $b_i = \sum_{j=1}^{i-1} p_j$ for $2 \leqslant i \leqslant N$. Let $s_i = \lceil -\log p_i \rceil$ for $1 \leqslant i \leqslant N$. Now define a code c by $c(a_i) = b_i^*$ where b_i^* is the (fractional part of the) binary expansion of b_i to s_i decimal places. Prove that this defines a decipherable code.

What does it mean for a code to be *optimal*? Is the code c defined in the previous paragraph in terms of the b_i^* necessarily optimal? Justify your answer.

Paper 2, Section II

12K Coding and Cryptography

(a) Define what it means to say that C is a *binary cyclic code*. Explain the bijection between the set of binary cyclic codes of length n and the factors of $X^n - 1$ in $\mathbb{F}_2[X]$.

(b) What is a *linear feedback shift register*?

Suppose that $M : \mathbb{F}_2^d \to \mathbb{F}_2^d$ is a linear feedback shift register. Further suppose $\mathbf{0} \neq \mathbf{x} \in \mathbb{F}_2^d$ and k is a positive integer such that $M^k\mathbf{x} = \mathbf{x}$. Let H be the $d \times k$ matrix $(\mathbf{x}, M\mathbf{x}, \ldots, M^{k-1}\mathbf{x})$. Considering H as a parity check matrix of a code C, show that C is a binary cyclic code.

(c) Suppose that C is a binary cyclic code. Prove that, if C does not contain the codeword $11\ldots1$, then all codewords in C have even weight.

Paper 1, Section I

3I Coding and Cryptography

(a) Briefly describe the methods of Shannon–Fano and of Huffman for the construction of prefix-free binary codes.

(b) In this part you are given that $-\log_2(1/10) \approx 3.32$, $-\log_2(2/10) \approx 2.32$, $-\log_2(3/10) \approx 1.74$ and $-\log_2(4/10) \approx 1.32$.

Let $\mathcal{A} = \{1, 2, 3, 4\}$. For $k \in \mathcal{A}$, suppose that the probability of choosing k is $k/10$.

(i) Find a Shannon–Fano code for this system and the expected word length.

(ii) Find a Huffman code for this system and the expected word length.

(iii) Verify that Shannon's noiseless coding theorem is satisfied in each case.

Paper 2, Section I

3I Coding and Cryptography

(a) Define the *information capacity* of a discrete memoryless channel (DMC).

(b) Consider a DMC where there are two input symbols, A and B, and three output symbols, A, B and $\star$. Suppose each input symbol is left intact with probability $1/2$, and transformed into a $\star$ with probability $1/2$.

(i) Write down the channel matrix, and calculate the information capacity.

(ii) Now suppose the output is further processed by someone who cannot distinguish between A and $\star$, so that the channel matrix becomes

$$\begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \end{pmatrix}.$$

Calculate the new information capacity.

Paper 3, Section I

3I Coding and Cryptography

Let N and p be very large positive integers with p a prime and $p > N$. The Chair of the Committee is able to inscribe pairs of very large integers on discs. The Chair wishes to inscribe a collection of discs in such a way that any Committee member who acquires r of the discs and knows the prime p can deduce the integer N, but owning $r - 1$ discs will give no information whatsoever. What strategy should the Chair follow?

[You may use without proof standard properties of the determinant of the $r \times r$ Vandermonde matrix.]

Paper 4, Section I

3I Coding and Cryptography

(a) What does it mean to say that a cipher has *perfect secrecy*? Show that if a cipher has perfect secrecy then there must be at least as many possible keys as there are possible plaintext messages. What is a *one-time pad*? Show that a one-time pad has perfect secrecy.

(b) I encrypt a binary sequence $a_1, a_2, \ldots, a_N$ using a one-time pad with key sequence $k_1, k_2, k_3, \ldots$. I transmit $a_1 + k_1, a_2 + k_2, \ldots, a_N + k_N$ to you. Then, by mistake, I also transmit $a_1 + k_2, a_2 + k_3, \ldots, a_N + k_{N+1}$ to you. Assuming that you know I have made this error, and that my message makes sense, how would you go about finding my message? Can you now decipher other messages sent using the same part of the key sequence? Briefly justify your answer.

Paper 1, Section II

11I Coding and Cryptography

(a) What does it mean to say that a binary code has *length* n, *size* M and *minimum distance* d?

Let $A(n, d)$ be the largest value of M for which there exists a binary $[n, M, d]$-code.

(i) Show that $A(n, 1) = 2^n$.

(ii) Suppose that $n, d > 1$. Show that if a binary $[n, M, d]$-code exists, then a binary $[n-1, M, d-1]$-code exists. Deduce that $A(n, d) \leqslant A(n-1, d-1)$.

(iii) Suppose that $n, d \geqslant 1$. Show that $A(n, d) \leqslant 2^{n-d+1}$.

(b) (i) For integers M and N with $0 \leqslant N \leqslant M$, show that

$$N(M-N) \leqslant \begin{cases} M^2/4, & \text{if } M \text{ is even,} \\ (M^2-1)/4, & \text{if } M \text{ is odd.} \end{cases}$$

For the remainder of this question, suppose that C is a binary $[n, M, d]$-code. For codewords $x = (x_1 \ldots x_n)$, $y = (y_1 \ldots y_n) \in C$ of length n, we define $x + y$ to be the word $((x_1 + y_1) \ldots (x_n + y_n))$ with addition modulo 2.

(ii) Explain why the Hamming distance $d(x, y)$ is the number of 1s in $x + y$.

(iii) Now we construct an $\binom{M}{2} \times n$ array A whose rows are all the words $x + y$ for pairs of distinct codewords x, y. Show that the number of 1s in A is at most

$$\begin{cases} nM^2/4, & \text{if } M \text{ is even,} \\ n(M^2-1)/4, & \text{if } M \text{ is odd.} \end{cases}$$

Show also that the number of 1s in A is at least $d\binom{M}{2}$.

(iv) Using the inequalities derived in part(b)(iii), deduce that if d is even and $n < 2d$ then

$$A(n, d) \leqslant 2 \left\lfloor \frac{d}{2d-n} \right\rfloor.$$

Paper 2, Section II

12I Coding and Cryptography

Let C be the Hamming $(n, n-d)$ code of weight 3, where $n = 2^d - 1$, $d > 1$. Let H be the parity-check matrix of C. Let $\nu(j)$ be the number of codewords of weight j in C.

(i) Show that for any two columns h_1 and h_2 of H there exists a unique third column h_3 such that $h_3 = h_2 + h_1$. Deduce that $\nu(3) = n(n-1)/6$.

(ii) Show that C contains a codeword of weight n.

(iii) Find formulae for $\nu(n-1)$, $\nu(n-2)$ and $\nu(n-3)$. Justify your answer in each case.

Paper 4, Section I

3G Coding and Cryptography

(a) Describe *Diffie-Hellman key exchange*. Why is it believed to be a secure system?

(b) Consider the following authentication procedure. Alice chooses public key N for the Rabin–Williams cryptosystem. To be sure we are in communication with Alice we send her a 'random item' $r \equiv m^2 \bmod N$. On receiving r, Alice proceeds to decode using her knowledge of the factorisation of N and finds a square root m_1 of r. She returns m_1 to us and we check $r \equiv m_1^2 \bmod N$. Is this authentication procedure secure? Justify your answer.

Paper 3, Section I

3G Coding and Cryptography

What does it mean to transmit reliably at rate R through a binary symmetric channel (BSC) with error probability p?

Assuming Shannon's second coding theorem (also known as Shannon's noisy coding theorem), compute the supremum of all possible reliable transmission rates of a BSC. Describe qualitatively the behaviour of the capacity as p varies. Your answer should address the following cases,

(i) p is small,

(ii) $p = 1/2$,

(iii) $p > 1/2$.

Paper 2, Section I

3G Coding and Cryptography

Define the *binary Hamming code* of length $n = 2^l - 1$ for $l \geqslant 3$. Define a *perfect code*. Show that a binary Hamming code is perfect.

What is the weight of the dual code of a binary Hamming code when $l = 3$?

Paper 1, Section I

3G Coding and Cryptography

Let X and Y be discrete random variables taking finitely many values. Define the *conditional entropy* $H(X|Y)$. Suppose Z is another discrete random variable taking values in a finite alphabet, and prove that

$$H(X|Y) \leqslant H(X|Y,Z) + H(Z).$$

[You may use the equality $H(X,Y) = H(X|Y) + H(Y)$ and the inequality $H(X|Y) \leqslant H(X)$.]

State and prove *Fano's inequality.*

Paper 1, Section II

11G Coding and Cryptography

What does it mean to say that C is a *binary linear code of length n, rank k and minimum distance d*? Let C be such a code.

(a) Prove that $n \geqslant d + k - 1$.

Let $x = (x_1, \ldots, x_n) \in C$ be a codeword with exactly d non-zero digits.

(b) Prove that puncturing C on the non-zero digits of x produces a code C' of length $n - d$, rank $k - 1$ and minimum distance d' for some $d' \geqslant \lceil \frac{d}{2} \rceil$.

(c) Deduce that $n \geqslant d + \sum_{1 \leqslant l \leqslant k-1} \lceil \frac{d}{2^l} \rceil$.

Paper 2, Section II

12G Coding and Cryptography

Describe the *Huffman coding scheme* and prove that Huffman codes are optimal.

Are the following statements true or false? Justify your answers.

(i) Given m messages with probabilities $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_m$ a Huffman coding will assign a unique set of word lengths.

(ii) An optimal code must be Huffman.

(iii) Suppose the m words of a Huffman code have word lengths $s_1, s_2, \ldots, s_m$. Then

$$\sum_{i=1}^{m} 2^{-s_i} = 1.$$

[*Throughout this question you may assume that a decipherable code with prescribed word lengths exists if and only if there is a prefix-free code with the same word lengths.*]

Paper 4, Section I

3H Coding & Cryptography

What is a *linear feedback shift register*? Explain the Berlekamp–Massey method for recovering a feedback polynomial of a linear feedback shift register from its output. Illustrate the method in the case when we observe output

$$0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\ldots.$$

Paper 3, Section I

3H Coding & Cryptography

Compute the rank and minimum distance of the cyclic code with generator polynomial $g(X) = X^3 + X^2 + 1$ and parity check polynomial $h(X) = X^4 + X^3 + X^2 + 1$. Now let α be a root of $g(X)$ in the field with 8 elements. We receive the word $r(X) = X^2 + X + 1 \pmod{X^7 - 1}$. Verify that $r(\alpha) = \alpha^4$, and hence decode $r(X)$ using minimum-distance decoding.

Paper 2, Section I

3H Coding & Cryptography

What is the channel matrix of a binary symmetric channel with error probability p?

State the maximum likelihood decoding rule and the minimum distance decoding rule. Prove that if $p < 1/2$, then they agree.

Let C be the repetition code $\{000, 111\}$. Suppose a codeword from C is sent through a binary symmetric channel with error probability p. Show that, if the minimum distance decoding rule is used, then the probability of error is $3p^2 - 2p^3$.

Paper 1, Section I

3H Coding & Cryptography

State and prove Shannon's noiseless coding theorem. [You may use Gibbs' and Kraft's inequalities as long as they are clearly stated.]

Paper 1, Section II

11H Coding & Cryptography

Define the *bar product* $C_1|C_2$ of binary linear codes C_1 and C_2, where C_2 is a subcode of C_1. Relate the rank and minimum distance of $C_1|C_2$ to those of C_1 and C_2 and justify your answer.

What is a *parity check* matrix for a linear code? If C_1 has parity check matrix P_1 and C_2 has parity check matrix P_2, find a parity check matrix for $C_1|C_2$.

Using the bar product construction, or otherwise, define the Reed–Muller code $RM(d,r)$ for $0 \leqslant r \leqslant d$. Compute the rank of $RM(d,r)$. Show that all but two codewords in $RM(d,1)$ have the same weight. Given d, for which r is it true that all elements of $RM(d,r)$ have even weight? Justify your answer.

Paper 2, Section II

12H Coding & Cryptography

Describe the RSA encryption scheme with public key (N,e) and private key d.

Suppose $N = pq$ with p and q distinct odd primes and $1 \leqslant x \leqslant N$ with x and N coprime. Denote the order of x in $\mathbb{F}_p^*$ by $\mathrm{O}_p(x)$. Further suppose $\Phi(N)$ divides $2^a b$ where b is odd. If $\mathrm{O}_p(x^b) \neq \mathrm{O}_q(x^b)$ prove that there exists $0 \leqslant t < a$ such that the greatest common divisor of $x^{2^t b} - 1$ and N is a nontrivial factor of N. Further, prove that the number of x satisfying $\mathrm{O}_p(x^b) \neq \mathrm{O}_q(x^b)$ is $\geqslant \Phi(N)/2$.

Hence, or otherwise, prove that finding the private key d from the public key (N,e) is essentially as difficult as factoring N.

Suppose a message m is sent using the RSA scheme with $e = 43$ and $N = 77$, and $c = 5$ is the received text. What is m?

An integer m satisfying $1 \leqslant m \leqslant N-1$ is called a *fixed point* if it is encrypted to itself. Prove that if m is a fixed point then so is $N - m$.

Paper 1, Section I

3G Coding & Cryptography

Let C be a binary code of length n. Define the following decoding rules: (i) *ideal observer*, (ii) *maximum likelihood*, (iii) *minimum distance*.

Let p denote the probability that a digit is mistransmitted and suppose $p < 1/2$. Prove that maximum likelihood and minimum distance decoding agree.

Suppose codewords 000 and 111 are sent with probabilities $4/5$ and $1/5$ respectively with error probability $p = 1/4$. If we receive 110, how should it be decoded according to the three decoding rules above?

Paper 2, Section I

3G Coding & Cryptography

Prove that a decipherable code with prescribed word lengths exists if and only if there is a prefix-free code with the same word lengths.

Paper 3, Section I

3G Coding & Cryptography

Find and describe all binary cyclic codes of length 7. Pair each code with its dual code. Justify your answer.

Paper 4, Section I

3G Coding & Cryptography

Describe the RSA system with public key (N, e) and private key d.

Give a simple example of how the system is vulnerable to a homomorphism attack.

Describe the El-Gamal signature scheme and explain how this can defeat a homomorphism attack.

Paper 1, Section II

10G Coding & Cryptography

Let C be a binary linear code. Explain what it means for C to have *length* n and *rank* k. Explain what it means for a codeword of C to have *weight* j.

Suppose C has length n, rank k, and A_j codewords of weight j. The weight enumerator polynomial of C is given by

$$W_C(s,t) = \sum_{j=0}^{n} A_j s^j t^{n-j}.$$

What is $W_C(1,1)$? Prove that $W_C(s,t) = W_C(t,s)$ if and only if $W_C(1,0) = 1$.

Define the *dual code* $C^\perp$ of C.

(i) Let $\mathbf{y} \in \mathbb{F}_2^n$. Show that

$$\sum_{\mathbf{x}\in C} (-1)^{\mathbf{x}.\mathbf{y}} = \begin{cases} 2^k, & \text{if } \mathbf{y} \in C^\perp, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) Extend the definition of weight to give a weight $w(\mathbf{y})$ for $\mathbf{y} \in \mathbb{F}_2^n$. Suppose that for t real and all $\mathbf{x} \in C$

$$\sum_{\mathbf{y}\in\mathbb{F}_2^n} t^{w(\mathbf{y})}(-1)^{\mathbf{x}.\mathbf{y}} = (1-t)^{w(\mathbf{x})}(1+t)^{n-w(\mathbf{x})}.$$

For s real, by evaluating

$$\sum_{\mathbf{x}\in C}\left(\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{\mathbf{x}.\mathbf{y}}\left(\frac{s}{t}\right)^{w(\mathbf{y})}\right)$$

in two different ways, show that

$$W_{C^\perp}(s,t) = 2^{-k} W_C(t-s, t+s).$$

Paper 2, Section II

11G Coding & Cryptography

Define the *entropy*, $H(X)$, of a random variable X. State and prove Gibbs' inequality.

Hence, or otherwise, show that $H(p_1, p_2, p_3) \leqslant H(p_1, 1-p_1)+(1-p_1)$ and determine when equality occurs.

Show that the Discrete Memoryless Channel with channel matrix

$$\begin{pmatrix} 1-\alpha-\beta & \alpha & \beta \\ \alpha & 1-\alpha-\beta & \beta \end{pmatrix}$$

has capacity $C = (1-\beta)(1-\log(1-\beta)) + (1-\alpha-\beta)\log(1-\alpha-\beta) + \alpha\log\alpha$.

Paper 1, Section I

3G Coding and Cryptography

Find the average length of an optimum decipherable binary code for a source that emits five words with probabilities

$$0.25,\ 0.15,\ 0.15,\ 0.2,\ 0.25.$$

Show that, if a source emits N words (with $N \geqslant 2$), and if $l_1, \ldots, l_N$ are the lengths of the codewords in an optimum encoding over the binary alphabet, then

$$l_1 + \cdots + l_N \leqslant \frac{1}{2}(N^2 + N - 2).$$

[*You may assume that an optimum encoding can be given by a Huffman encoding.*]

Paper 2, Section I

3G Coding and Cryptography

Show that the binary channel with channel matrix

$$\begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

has capacity $\log 5 - 2$.

Paper 3, Section I

3G Coding and Cryptography

Describe in words the *unicity distance* of a cryptosystem.

Denote the cryptosystem by $\langle M, K, C \rangle$, in the usual way, and let $m \in M$ and $k \in K$ be random variables and $c = e(m, k)$. The unicity distance U is formally defined to be the least $n > 0$ such that $H(k|c^{(n)}) = 0$. Derive the formula

$$U = \frac{\log |K|}{\log |\Sigma| - H},$$

where $H = H(m)$, and Σ is the alphabet of the ciphertext. Make clear any assumptions you make.

The *redundancy* of a language is given by $R = 1 - \frac{H}{\log |\Sigma|}$. If a language has zero redundancy what is the unicity of any cryptosystem?

Paper 4, Section I

3G Coding and Cryptography

Describe the Rabin–Williams scheme for coding a message x as x^2 modulo a certain N. Show that, if N is chosen appropriately, breaking this code is equivalent to factorising the product of two primes.

Paper 1, Section II

10G Coding and Cryptography

What does it mean to say a binary code C has *length* n, *size* m and *minimum distance* d?

Let $A(n,d)$ be the largest value of m for which there exists an $[n,m,d]$-code. Prove that

$$\frac{2^n}{V(n,d-1)} \leqslant A(n,d) \leqslant \frac{2^n}{V(n,\lfloor (d-1)/2 \rfloor)},$$

where

$$V(n,r) = \sum_{j=0}^{r} \binom{n}{j}.$$

Another bound for $A(n,d)$ is the Singleton bound given by

$$A(n,d) \leqslant 2^{n-d+1}.$$

Prove the Singleton bound and give an example of a linear code of length $n > 1$ that satisfies $A(n,d) = 2^{n-d+1}$.

Paper 2, Section II

11G Coding and Cryptography

Define a *BCH code* of length n, where n is odd, over the field of 2 elements with design distance δ. Show that the minimum weight of such a code is at least δ. [Results about the Vandermonde determinant may be quoted without proof, provided they are stated clearly.]

Let $\omega \in \mathbb{F}_{16}$ be a root of $X^4 + X + 1$. Let C be the BCH code of length 15 with defining set $\{\omega, \omega^2, \omega^3, \omega^4\}$. Find the generator polynomial of C and the rank of C. Determine the error positions of the following received words:

(i) $r(X) = 1 + X^6 + X^7 + X^8$,

(ii) $r(X) = 1 + X + X^4 + X^5 + X^6 + X^9$.

Paper 4, Section I

3G Coding and Cryptography

Explain how to construct binary Reed–Muller codes. State and prove a result giving the minimum distance for each such Reed–Muller code.

Paper 3, Section I

3G Coding and Cryptography

Let A be a random variable that takes each value a in the finite alphabet $\mathcal{A}$ with probability $p(a)$. Show that, if each $l(a)$ is an integer greater than 0 and $\sum 2^{-l(a)} \leqslant 1$, then there is a decodable binary code $c : \mathcal{A} \to \{0,1\}^*$ with each codeword $c(a)$ having length $l(a)$.

Prove that, for any decodable code $c : \mathcal{A} \to \{0,1\}^*$, we have

$$H(A) \leqslant \mathbb{E}\, l(A)$$

where $H(A)$ is the entropy of the random variable A. When is there equality in this inequality?

Paper 2, Section I

3G Coding and Cryptography

A random variable A takes values in the alphabet $\mathcal{A} = \{a, b, c, d, e\}$ with probabilities 0.4, 0.2, 0.2, 0.1 and 0.1. Calculate the entropy of A.

Define what it means for a code for a general finite alphabet to be *optimal*. Find such a code for the distribution above and show that there are optimal codes for this distribution with differing lengths of codeword.

[You may use any results from the course without proof. Note that $\log_2 5 \simeq 2.32$.]

Paper 1, Section I

3G Coding and Cryptography

Let $\mathcal{A}$ be a finite alphabet. Explain what is meant by saying that a binary code $c : \mathcal{A} \to \{0,1\}^*$ has *minimum distance* δ. If c is such a binary code with minimum distance δ, show that c is $\delta - 1$ error-detecting and $\lfloor \frac{1}{2}(\delta - 1) \rfloor$ error-correcting.

Show that it is possible to construct a code that has minimum distance δ for any integer $\delta > 0$.

Paper 1, Section II

9G Coding and Cryptography

Define the *Hamming code*. Show that it is a perfect, linear, 1-error correcting code.

I wish to send a message through a noisy channel to a friend. The message consists of a large number $N = 1,000$ of letters from a 16-letter alphabet $\mathcal{A}$. When my friend has decoded the message, she can tell whether there have been any errors. If there have, she asks me to send the message again and this is repeated until she has received the message without error. For each individual binary digit that is transmitted, there is independently a small probability $p = 0.001$ of an error.

(a) Suppose that I encode my message by writing each letter as a 4-bit binary string. The whole message is then $4N$ bits long. What is the probability P that the entire message is transmitted without error? How many times should I expect to transmit the message until my friend receives it without error?

(b) As an alternative, I use the Hamming code to encode each letter of $\mathcal{A}$ as a 7-bit binary string. What is the probability that my friend can decode a single 7-bit string correctly? Deduce that the probability Q that the entire message is correctly decoded is given approximately by

$$Q \simeq (1 - 21p^2)^N \simeq \exp(-21Np^2)\,.$$

Which coding method is better?

Paper 2, Section II

10G Coding and Cryptography

Briefly describe the *RSA public key cipher*.

Just before it went into liquidation, the Internet Bank decided that it wanted to communicate with each of its customers using an RSA cipher. So, it chose a large modulus N, which is the product of two large prime numbers, and chose encrypting exponents e_j and decrypting exponents d_j for each customer j. The bank published N and e_j and sent the decrypting exponent d_j secretly to customer j. Show explicitly that the cipher can be broken by each customer.

The bank sent out the same message to each customer. I am not a customer of the bank but have two friends who are and I notice that their published encrypting exponents are coprime. Explain how I can find the original message. Can I break the cipher?

Paper 4, Section I

4I Coding and Cryptography

Explain what is meant by a *Bose–Ray Chaudhuri–Hocquenghem (BCH) code with design distance* δ. Prove that, for such a code, the minimum distance between code words is at least δ. How many errors will the code detect? How many errors will it correct?

Paper 3, Section I

4I Coding and Cryptography

Let A be a random variable that takes values in the finite alphabet $\mathcal{A}$. Prove that there is a decodable binary code $c : \mathcal{A} \to \{0,1\}^*$ that satisfies

$$H(A) \leqslant \mathbb{E}(l(A)) \leqslant H(A) + 1 \ ,$$

where $l(a)$ is the length of the code word $c(a)$ and $H(A)$ is the entropy of A.

Is it always possible to find such a code with $\mathbb{E}(l(A)) = H(A)$? Justify your answer.

Paper 2, Section I

4I Coding and Cryptography

Let $c : \mathcal{A} \to \{0,1\}^*$ be a decodable binary code defined on a finite alphabet $\mathcal{A}$. Let $l(a)$ be the length of the code word $c(a)$. Prove that

$$\sum_{a \in \mathcal{A}} 2^{-l(a)} \leqslant 1 \ .$$

Show that, for the decodable code $c : \mathcal{A} \to \{0,1\}^*$ described above, there is a prefix-free code $p : \mathcal{A} \to \{0,1\}^*$ with each code word $p(a)$ having length $l(a)$. [You may use, without proof, any standard results from the course.]

Paper 1, Section I

4I Coding and Cryptography

State and prove Gibbs' inequality.

Show that, for a pair of discrete random variables X and Y, each taking finitely many values, the joint entropy $H(X,Y)$ satisfies

$$H(X,Y) \leqslant H(X) + H(Y) \ ,$$

with equality precisely when X and Y are independent.

Paper 2, Section II

12I Coding and Cryptography

What is the *information capacity* of a memoryless, time-independent channel? Compute the information capacity of a binary symmetric channel with probability p of error. Show the steps in your computation.

Binary digits are transmitted through a noisy channel, which is memoryless and time-independent. With probability α $(0 < \alpha < 1)$ the digit is corrupted and noise is received, otherwise the digit is transmitted unchanged. So, if we denote the input by 0 and 1 and the output as 0, $*$ and 1 with $*$ denoting the noise, the transition matrix is

$$\begin{pmatrix} 1-\alpha & 0 \\ \alpha & \alpha \\ 0 & 1-\alpha \end{pmatrix} \ .$$

Compute the information capacity of this channel.

Explain how to code a message for transmission through the channel described above, and how to decode it, so that the probability of error for each bit is arbitrarily small.

Paper 1, Section II

12I Coding and Cryptography

Describe, briefly, either the RSA or the Elgamal public key cipher. You should explain, without proof, why it is believed to be difficult to break the cipher you describe.

How can such a cipher be used to sign messages? You should explain how the intended recipient of the message can (a) know from whom it came; (b) know that the message has not been changed; and (c) demonstrate that the sender must have signed it.

Let $I_0, I_1, \ldots, I_N$ be friendly individuals each of whom has a public key cipher. I_0 wishes to send a message to I_N by passing it first to I_1, then I_1 passes it to I_2, I_2 to I_3, until finally it is received by I_N. At each stage the message can be modified to show from whom it was received and to whom it is sent. Devise a way in which these modifications can be made so that I_N can be confident both of the content of the original message and that the message has been passed through the intermediaries $I_1, I_2, \ldots, I_{N-1}$ in that order and has not been modified by an enemy agent. Assume that it takes a negligible time to transmit a message from I_k to I_{k+1} for each k, but the time needed to modify a message is not negligible.

Paper 4, Section I

4H Coding and Cryptography

Describe how a stream cipher works. What is a one-time pad?

A one-time pad is used to send the message $x_1x_2x_3x_4x_5x_6y_7$ which is encoded as 0101011. In error, it is reused to send the message $y_0x_1x_2x_3x_4x_5x_6$ which is encoded as 0100010. Show that there are two possibilities for the substring $x_1x_2x_3x_4x_5x_6$, and find them.

Paper 3, Section I

4H Coding and Cryptography

Describe briefly the Rabin cipher with modulus N, explaining how it can be deciphered by the intended recipient and why it is difficult for an eavesdropper to decipher it.

The Cabinet decides to communicate using Rabin ciphers to maintain confidentiality. The Cabinet Secretary encrypts a message, represented as a positive integer m, using the Rabin cipher with modulus N (with $0 < m < N$) and publishes both the encrypted message and the modulus. The Defence Secretary deciphers this message to read it but then foolishly encrypts it again using a Rabin cipher with a different modulus N' (with $m < N'$) and publishes the newly encrypted message and N'. Mr Rime (the Leader of the Opposition) knows this has happened. Explain how Rime can work out what the original message was using the two different encrypted versions.

Can Rime decipher other messages sent out by the Cabinet using the original modulus N?

Paper 2, Section I

4H Coding and Cryptography

Let $A(n, d)$ denote the maximum size of a binary code of length n with minimum distance d. For fixed δ with $0 < \delta < 1/2$, let $\alpha(\delta) = \limsup \frac{1}{n} \log_2 A(n, n\delta)$. Show that

$$1 - H(\delta) \leqslant \alpha(\delta) \leqslant 1 - H(\delta/2)$$

where $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$.

[You may assume the GSV and Hamming bounds and any form of Stirling's theorem provided you state them clearly.]

Paper 1, Section I

4H Coding and Cryptography

A binary Huffman code is used for encoding symbols $1, \ldots, m$ occurring with respective probabilities $p_1 \geqslant \cdots \geqslant p_m > 0$ where $\sum_{1 \leqslant j \leqslant m} p_j = 1$. Let s_1 be the length of a shortest codeword and s_m the length of a longest codeword. Determine the maximal and minimal values of each of s_1 and s_m, and find binary trees for which they are attained.

Paper 2, Section II

12H Coding and Cryptography

Define a BCH code of length n, where n is odd, over the field of 2 elements with design distance δ. Show that the minimum weight of such a code is at least δ. [Results about the van der Monde determinant may be quoted without proof, provided they are stated clearly.]

Consider a BCH code of length 31 over the field of 2 elements with design distance 8. Show that the minimum distance is at least 11. [*Hint: Let α be a primitive element in the field of 2^5 elements, and consider the minimal polynomial for certain powers of α.*]

Paper 1, Section II

12H Coding and Cryptography

Define the *bar product* $C_1|C_2$ of binary linear codes C_1 and C_2, where C_2 is a subcode of C_1. Relate the rank and minimum distance of $C_1|C_2$ to those of C_1 and C_2 and justify your answer. Show that if $C^\perp$ denotes the dual code of C, then

$$(C_1|C_2)^\perp = C_2^\perp | C_1^\perp \, .$$

Using the bar product construction, or otherwise, define the Reed–Muller code $\mathrm{RM}(d, r)$ for $0 \leqslant r \leqslant d$. Show that if $0 \leqslant r \leqslant d-1$, then the dual of $\mathrm{RM}(d, r)$ is again a Reed–Muller code.

Paper 4, Section I

4G Coding and Cryptography

Describe the BB84 protocol for quantum key exchange.

Suppose we attempt to implement the BB84 protocol but cannot send single photons. Instead we send K photons at a time all with the same polarization. An enemy can separate one of these photons from the other $K-1$. Explain briefly how the enemy can intercept the key exchange without our knowledge.

Show that an enemy can find our common key if $K=3$. Can she do so when $K=2$ (with suitable equipment)?

Paper 3, Section I

4G Coding and Cryptography

Describe the RSA system with public key (N, e) and private key d. Give a simple example of how the system is vulnerable to a homomorphism attack. Explain how a signature system prevents such an attack.

Paper 2, Section I

4G Coding and Cryptography

What is a (binary) linear code? What does it mean to say that a linear code has length n and minimum weight d? When is a linear code perfect? Show that, if $n=2^r-1$, there exists a perfect linear code of length n and minimum weight 3.

Paper 1, Section I

4G Coding and Cryptography

Let $\mathcal{A}$ and $\mathcal{B}$ be alphabets of sizes m and a respectively. What does it mean to say that $c : \mathcal{A} \to \mathcal{B}^*$ is a decodable code? State Kraft's inequality.

Suppose that a source emits letters from the alphabet $\mathcal{A} = \{1, 2, \ldots, m\}$, each letter j occurring with (known) probability $p_j > 0$. Let S be the codeword-length random variable for a decodable code $c : \mathcal{A} \to \mathcal{B}^*$, where $|\mathcal{B}| = a$. It is desired to find a decodable code that minimizes the expected value of a^S. Establish the lower bound $\mathbb{E}(a^S) \geqslant (\sum_{j=1}^m \sqrt{p_j})^2$, and characterise when equality occurs. [*Hint. You may use without proof the Cauchy-Schwarz inequality, that (for positive x_i, y_i)*

$$\sum_{i=1}^m x_i y_i \leqslant (\sum_{i=1}^m x_i^2)^{1/2} (\sum_{i=1}^m y_i^2)^{1/2} ,$$

with equality if and only if $x_i = \lambda y_i$ for all i.]

Paper 2, Section II

12G Coding and Cryptography

What does it mean to say that $f : \mathbb{F}_2^d \to \mathbb{F}_2^d$ is a linear feedback shift register? Let $(x_n)_{n \geqslant 0}$ be a stream produced by such a register. Show that there exist N, M with $N + M \leqslant 2^d - 1$ such that $x_{r+N} = x_r$ for all $r \geqslant M$.

Describe and justify the Berlekamp–Massey method for 'breaking' a cipher stream arising from a linear feedback register of unknown length.

Let x_n, y_n, z_n be three streams produced by linear feedback registers. Set

$$k_n = x_n \quad \text{if } y_n = z_n$$

$$k_n = y_n \quad \text{if } y_n \neq z_n .$$

Show that k_n is also a stream produced by a linear feedback register. Sketch proofs of any theorems you use.

Paper 1, Section II

12G Coding and Cryptography

Define a cyclic binary code of length n.

Show how codewords can be identified with polynomials in such a way that cyclic binary codes correspond to ideals in the polynomial ring with a suitably chosen multiplication rule.

Prove that any cyclic binary code C has a unique generator, that is, a polynomial $c(X)$ of minimum degree, such that the code consists of the multiples of this polynomial. Prove that the rank of the code equals $n - \deg c(X)$, and show that $c(X)$ divides $X^n - 1$.

Show that the repetition and parity check codes are cyclic, and determine their generators.

Paper 1, Section I

4G Coding and Cryptography

I think of an integer n with $1 \leqslant n \leqslant 10^6$. Explain how to find n using twenty questions (or less) of the form 'Is it true that $n \geqslant m$?' to which I answer yes or no.

I have watched a horse race with 15 horses. Is it possible to discover the order in which the horses finished by asking me twenty questions to which I answer yes or no?

Roughly how many questions of the yes/no type are required to discover the order in which n horses finished if n is large?

[You may assume that I answer honestly.]

Paper 2, Section I

4G Coding and Cryptography

I happen to know that an apparently fair coin actually has probability p of heads with $1 > p > 1/2$. I play a very long sequence of games of heads and tails in which my opponent pays me back twice my stake if the coin comes down heads and takes my stake if the coin comes down tails. I decide to bet a proportion α of my fortune at the end of the nth game in the $(n+1)$st game. Determine, giving justification, the value α_0 maximizing the expected logarithm of my fortune in the long term, assuming I use the same α_0 at each game. Can it be actually disadvantageous for me to choose an $\alpha < \alpha_0$ (in the sense that I would be better off not playing)? Can it be actually disadvantageous for me to choose an $\alpha > \alpha_0$?

[Moral issues should be ignored.]

Paper 3, Section I

4G Coding and Cryptography

What is the rank of a binary linear code C? What is the weight enumeration polynomial W_C of C?

Show that $W_C(1,1) = 2^r$ where r is the rank of C. Show that $W_C(s,t) = W_C(t,s)$ for all s and t if and only if $W_C(1,0) = 1$.

Find, with reasons, the weight enumeration polynomial of the repetition code of length n, and of the simple parity check code of length n.

Paper 4, Section I

4G Coding and Cryptography

Describe a scheme for sending messages based on quantum theory which is not vulnerable to eavesdropping. You may ignore engineering problems.

Paper 1, Section II

12G Coding and Cryptography

Describe the Rabin–Williams coding scheme. Show that any method for breaking it will enable us to factorise the product of two primes.

Explain how the Rabin–Williams scheme can be used for bit sharing (that is to say 'tossing coins by phone').

Paper 2, Section II

12G Coding and Cryptography

Define a cyclic code. Show that there is a bijection between the cyclic codes of length n and the factors of $X^n - 1$ over the field $\mathbb{F}_2$ of order 2.

What is meant by saying that α is a primitive nth root of unity in a finite field extension K of $\mathbb{F}_2$? What is meant by saying that C is a BCH code of length n with defining set $\{\alpha, \alpha^2, \ldots, \alpha^{\delta-1}\}$? Show that such a code has minimum distance at least δ.

Suppose that K is a finite field extension of $\mathbb{F}_2$ in which $X^7 - 1$ factorises into linear factors. Show that if β is a root of $X^3 + X^2 + 1$ then β is a primitive 7th root of unity and β^2 is also a root of $X^3 + X^2 + 1$. Quoting any further results that you need show that the BCH code of length 7 with defining set $\{\beta, \beta^2\}$ is the Hamming code.

[Results on the Vandermonde determinant may be used without proof provided they are quoted correctly.]

Paper 1, Section I

4H Coding and Cryptography

Explain what is meant by saying that a binary code $\mathcal{C}$ is a decodable code with words C_j of length l_j for $1 \leqslant j \leqslant n$. Prove the MacMillan inequality which states that, for such a code,

$$\sum_{j=1}^{n} 2^{-l_j} \leqslant 1 .$$

Paper 2, Section I

4H Coding and Cryptography

Describe the standard Hamming code of length 7, proving that it corrects a single error. Find its weight enumeration polynomial.

Paper 3, Section I

4H Coding and Cryptography

What is a linear code? What is a parity check matrix for a linear code? What is the minimum distance $d(C)$ for a linear code C?

If C_1 and C_2 are linear codes having a certain relation (which you should specify), define the bar product $C_1 | C_2$. Show that

$$d(C_1 | C_2) = \min \left\{ 2d(C_1), d(C_2) \right\} .$$

If C_1 has parity check matrix P_1 and C_2 has parity check matrix P_2, find a parity check matrix for $C_1 | C_2$.

Paper 4, Section I

4H Coding and Cryptography

What is the discrete logarithm problem?

Describe the Diffie–Hellman key exchange system for two people. What is the connection with the discrete logarithm problem? Why might one use this scheme rather than just a public key system or a classical (pre-1960) coding system?

Extend the Diffie–Hellman system to n people using $n(n-1)$ transmitted numbers.

Paper 1, Section II

12H Coding and Cryptography

State and prove Shannon's theorem for the capacity of a noisy memoryless binary symmetric channel, defining the terms you use.

[You may make use of any form of Stirling's formula and any standard theorems from probability, provided that you state them exactly.]

Paper 2, Section II

12H Coding and Cryptography

The Van der Monde matrix $V(x_0, x_1, \ldots, x_{r-1})$ is the $r \times r$ matrix with (i,j)th entry x_{i-1}^{j-1}. Find an expression for $\det V(x_0, x_1, \ldots, x_{r-1})$ as a product. Explain why this expression holds if we work modulo p a prime.

Show that $\det V(x_0, x_1, \ldots, x_{r-1}) \equiv 0$ modulo p if $r > p$, and that there exist $x_0, \ldots, x_{p-1}$ such that $\det V(x_0, x_1, \ldots, x_{p-1}) \not\equiv 0$. By using Wilson's theorem, or otherwise, find the possible values of $\det V(x_0, x_1, \ldots, x_{p-1})$ modulo p.

The Dark Lord Y'Trinti has acquired the services of the dwarf Trigon who can engrave pairs of very large integers on very small rings. The Dark Lord wishes Trigon to engrave n rings in such a way that anyone who acquires r of the rings and knows the Prime Perilous p can deduce the Integer N of Power, but owning $r-1$ rings will give no information whatsoever. The integers N and p are very large and $p > N$. Advise the Dark Lord.

For reasons to be explained in the prequel, Trigon engraves an $(n+1)$st ring with random integers. A band of heroes (who know the Prime Perilous and all the information contained in this question) set out to recover the rings. What, if anything, can they say, with very high probability, about the Integer of Power if they have r rings (possibly including the fake)? What can they say if they have $r+1$ rings? What if they have $r+2$ rings?

Paper 1, Section I

4H Coding and Cryptography

I am putting up my Christmas lights. If I plug in a set of bulbs and one is defective, none will light up. A badly written note left over from the previous year tells me that exactly one of my 10 bulbs is defective and that the probability that the kth bulb is defective is $k/55$.

(i) Find an explicit procedure for identifying the defective bulb in the least expected number of steps.

[You should explain your method but no proof is required.]

(ii) Is there a different procedure from the one you gave in (i) with the same expected number of steps? Either write down another procedure and explain briefly why it gives the same expected number or explain briefly why no such procedure exists.

(iii) Because I make such a fuss about each test, my wife wishes me to tell her the maximum number N of trials that might be required. Will the procedure in (i) give the minimum N? Either write down another procedure and explain briefly why it gives a smaller N or explain briefly why no such procedure exists.

Paper 2, Section I

4H Coding and Cryptography

Knowing that

$$25 \equiv 2886^2 \mod 3953$$

and that 3953 is the product of two primes p and q, find p and q.

[You should explain your method in sufficient detail to show that it is reasonably general.]

Paper 3, Section I

4H Coding and Cryptography

Define a binary code of length 15 with information rate 11/15 which will correct single errors. Show that it has the rate stated and give an explicit procedure for identifying the error. Show that the procedure works.

[*Hint: You may wish to imitate the corresponding discussion for a code of length* 7 .]

Paper 4, Section I

4H Coding and Cryptography

What is a *general feedback register*? What is a *linear feedback register*? Give an example of a general feedback register which is not a linear feedback register and prove that it has the stated property.

By giving proofs or counterexamples, establish which, if any, of the following statements are true and which, if any, are false.

(i) Given two linear feedback registers, there always exist non-zero initial fills for which the outputs are identical.

(ii) If two linear feedback registers have different lengths, there do not exist non-zero initial fills for which the outputs are identical.

(iii) If two linear feedback registers have different lengths, there exist non-zero initial fills for which the outputs are not identical.

(iv) There exist two linear feedback registers of different lengths and non-zero initial fills for which the outputs are identical.

Paper 1, Section II

12H Coding and Cryptography

(i) State and prove Gibbs' inequality.

(ii) A casino offers me the following game: I choose strictly positive numbers $a_1, \ldots, a_n$ with $\sum_{j=1}^n a_j = 1$. I give the casino my entire fortune f and roll an n-sided die. With probability p_j the casino returns $u_j^{-1} a_j f$ for $j = 1, 2, \ldots, n$. If I intend to play the game many times (staking my entire fortune each time) explain carefully why I should choose $a_1, \ldots, a_n$ to maximise $\sum_{j=1}^n p_j \log(u_j^{-1} a_j)$.

[You should assume $n \geqslant 2$ and $u_j, p_j > 0$ for each j.]

(iii) Determine the appropriate $a_1, \ldots, a_n$. Let $\sum_{i=1}^n u_i = U$. Show that, if $U < 1$, then, in the long run with high probability, my fortune increases. Show that, if $U > 1$, the casino can choose $u_1, \ldots, u_n$ in such a way that, in the long run with high probability, my fortune decreases. Is it true that, if $U > 1$, any choice of $u_1, \ldots, u_n$ will ensure that, in the long run with high probability, my fortune decreases? Why?

Paper 2, Section II

12H Coding and Cryptography

Describe the construction of the Reed–Miller code $RM(m, d)$. Establish its information rate and minimum weight.

Show that every codeword in $RM(d, d-1)$ has even weight. By considering $\mathbf{x} \wedge \mathbf{y}$ with $\mathbf{x} \in RM(m, r)$ and $\mathbf{y} \in RM(m, m-r-1)$, or otherwise, show that $RM(m, m-r-1) \subseteq RM(m, r)^\perp$. Show that, in fact, $RM(m, m-r-1) = RM(m, r)^\perp$.

1/I/4G **Coding and Cryptography**

Define the entropy $H(X)$ of a random variable X that takes no more than N different values. What are the maximum and the minimum values for the entropy for a fixed value of N? Explain when the maximum and minimum are attained. You should prove any inequalities that you use.

2/I/4G **Coding and Cryptography**

Describe briefly the Shannon–Fano and Huffman binary codes for a finite alphabet. Find examples of such codes for the alphabet $\mathcal{A} = \{a, b, c, d\}$ when the four letters are taken with probabilities $0.4, 0.3, 0.2$ and 0.1 respectively.

1/II/12G **Coding and Cryptography**

State Shannon's Noisy Coding Theorem for a binary symmetric channel.

Define the *mutual information* of two discrete random variables X and Y. Prove that the mutual information is symmetric and non-negative. Define also the *information capacity* of a channel.

A channel transmits numbers chosen from the alphabet $\mathcal{A} = \{0, 1, 2\}$ and has transition matrix

$$\begin{pmatrix} 1-2\beta & \beta & \beta \\ \beta & 1-2\beta & \beta \\ \beta & \beta & 1-2\beta \end{pmatrix}$$

for a number β with $0 \leqslant \beta \leqslant \frac{1}{3}$. Calculate the information capacity of the channel.

3/I/4G **Coding and Cryptography**

Define the Hamming code $h : \mathbb{F}_2^4 \to \mathbb{F}_2^7$ and prove that the minimum distance between two distinct code words is 3. Explain how the Hamming code allows one error to be corrected.

A new code $c : \mathbb{F}_2^4 \to \mathbb{F}_2^8$ is obtained by using the Hamming code for the first 7 bits and taking the last bit as a check digit on the previous 7. Find the minimum distance between two distinct code words for this code. How many errors can this code detect? How many errors can it correct?

2/II/12G **Coding and Cryptography**

Describe the Rabin cipher with modulus N, explaining how it can be deciphered by the intended recipient and why it is difficult for an interceptor to decipher it.

The Bursars' Committee decides to communicate using Rabin ciphers to maintain confidentiality. The secretary of the committee encrypts a message, thought of as a positive integer m, using the Rabin cipher with modulus N (with $0 < m < N$) and publishes both the encrypted message and the modulus. A foolish bursar deciphers this message to read it but then encrypts it again using a Rabin cipher with a different modulus N' (with $m < N'$) and publishes the newly encrypted message and N'. The president of CUSU, who happens to be a talented mathematician, knows that this has happened. Explain how the president can work out what the original message was using the two different encrypted versions.

Can the president of CUSU also decipher other messages sent out by the Bursars' Committee?

4/I/4G **Coding and Cryptography**

What is a binary *cyclic* code of length N? What is the generator polynomial for such a cyclic code? Prove that the generator polynomial is a factor of $X^N - 1$ over the field $\mathbb{F}_2$.

Find all the binary cyclic codes of length 5 .

1/I/4G **Coding and Cryptography**

Let Σ_1 and Σ_2 be alphabets of sizes m and a. What does it mean to say that $f : \Sigma_1 \to \Sigma_2^*$ is a decipherable code? State the inequalities of Kraft and Gibbs, and deduce that if letters are drawn from Σ_1 with probabilities $p_1, \ldots, p_m$ then the expected word length is at least $H(p_1, \ldots, p_m)/\log a$.

2/I/4G **Coding and Cryptography**

Briefly explain how and why a signature scheme is used. Describe the El Gamal scheme.

1/II/11G **Coding and Cryptography**

Define the bar product $C_1|C_2$ of linear codes C_1 and C_2, where C_2 is a subcode of C_1. Relate the rank and minimum distance of $C_1|C_2$ to those of C_1 and C_2. Show that if $C^\perp$ denotes the dual code of C, then

$$(C_1|C_2)^\perp = C_2^\perp|C_1^\perp.$$

Using the bar product construction, or otherwise, define the Reed–Muller code $RM(d, r)$ for $0 \leqslant r \leqslant d$. Show that if $0 \leqslant r \leqslant d-1$, then the dual of $RM(d, r)$ is again a Reed–Muller code.

3/I/4G **Coding and Cryptography**

Compute the rank and minimum distance of the cyclic code with generator polynomial $g(X) = X^3 + X + 1$ and parity-check polynomial $h(X) = X^4 + X^2 + X + 1$. Now let α be a root of $g(X)$ in the field with 8 elements. We receive the word $r(X) = X^5 + X^3 + X \pmod{X^7 - 1}$. Verify that $r(\alpha) = \alpha^4$, and hence decode $r(X)$ using minimum-distance decoding.

2/II/11G **Coding and Cryptography**

Define the capacity of a discrete memoryless channel. State Shannon's second coding theorem and use it to show that the discrete memoryless channel with channel matrix

$$\begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

has capacity $\log 5 - 2$.

4/I/4G **Coding and Cryptography**

What is a linear feedback shift register? Explain the Berlekamp–Massey method for recovering the feedback polynomial of a linear feedback shift register from its output. Illustrate in the case when we observe output

1 0 1 0 1 1 0 0 1 0 0 0 ....

1/I/4G **Coding and Cryptography**

Define a linear feedback shift register. Explain the Berlekamp–Massey method for "breaking" a key stream produced by a linear feedback shift register of unknown length. Use it to find the feedback polynomial of a linear feedback shift register with output sequence

$$0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\ \ldots.$$

2/I/4G **Coding and Cryptography**

Let Σ_1 and Σ_2 be alphabets of sizes m and a. What does it mean to say that an a-ary code $f : \Sigma_1 \to \Sigma_2^*$ is decipherable? Show that if f is decipherable then the word lengths $s_1, \ldots, s_m$ satisfy

$$\sum_{i=1}^{m} a^{-s_i} \leqslant 1\ .$$

Find a decipherable binary code consisting of codewords 011, 0111, 01111, 11111, and three further codewords of length 2. How do you know the example you have given is decipherable?

2/II/12G **Coding and Cryptography**

Define a cyclic code. Show that there is a bijection between the cyclic codes of length n, and the factors of $X^n - 1$ in $\mathbb{F}_2[X]$.

If n is an odd integer then we can find a finite extension K of $\mathbb{F}_2$ that contains a primitive nth root of unity α. Show that a cyclic code of length n with defining set $\{\alpha, \alpha^2, \ldots, \alpha^{\delta-1}\}$ has minimum distance at least δ. Show that if $n = 7$ and $\delta = 3$ then we obtain Hamming's original code.

[*You may quote a formula for the Vandermonde determinant without proof.*]

3/I/4G **Coding and Cryptography**

What does it mean to say that a binary code C has length n, size m and minimum distance d? Let $A(n, d)$ be the largest value of m for which there exists an $[n, m, d]$-code. Prove that

$$\frac{2^n}{V(n, d-1)} \leqslant A(n, d) \leqslant \frac{2^n}{V(n, \lfloor \frac{1}{2}(d-1) \rfloor)}$$

where $V(n, r) = \sum_{j=0}^{r} \binom{n}{j}$.

3/II/12G **Coding and Cryptography**

Describe the RSA system with public key (N, e) and private key (N, d). Briefly discuss the possible advantages or disadvantages of taking (i) $e = 2^{16}+1$ or (ii) $d = 2^{16}+1$.

Explain how to factor N when both the private key and public key are known.

Describe the bit commitment problem, and briefly indicate how RSA can be used to solve it.

4/I/4G **Coding and Cryptography**

A binary erasure channel with erasure probability p is a discrete memoryless channel with channel matrix

$$\begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix} .$$

State Shannon's second coding theorem, and use it to compute the capacity of this channel.

1/I/4J **Coding and Cryptography**

Briefly describe the methods of Shannon-Fano and Huffman for economical coding. Illustrate both methods by finding decipherable binary codings in the case where messages $\mu_1, \ldots, \mu_5$ are emitted with probabilities $0.45, 0.25, 0.2, 0.05, 0.05$. Compute the expected word length in each case.

2/I/4J **Coding and Cryptography**

What is a *linear binary code*? What is the *weight* $w(C)$ of a linear binary code C? Define the bar product $C_1|C_2$ of two binary linear codes C_1 and C_2, stating the conditions that C_1 and C_2 must satisfy. Under these conditions show that

$$w(C_1|C_2) \geqslant \min(2w(C_1), w(C_2)).$$

2/II/12J **Coding and Cryptography**

What does it means to say that $f : \mathbb{F}_2^d \to \mathbb{F}_2^d$ is a linear feedback shift register? Let $(x_n)_{n\geqslant 0}$ be a stream produced by such a register. Show that there exist N, M with $N + M \leqslant 2^d - 1$ such that $x_{r+N} = x_r$ for all $r \geqslant M$.

Explain and justify the Berlekamp–Massey method for 'breaking' a cipher stream arising from a linear feedback register of unknown length.

Let x_n, y_n, z_n be three streams produced by linear feedback registers. Set

$$k_n = x_n \text{ if } y_n = z_n$$

$$k_n = y_n \text{ if } y_n \neq z_n\,.$$

Show that k_n is also a stream produced by a linear feedback register. Sketch proofs of any theorems that you use.

3/I/4J **Coding and Cryptography**

Briefly explain how and why a signature scheme is used. Describe the el Gamal scheme.

3/II/12J **Coding and Cryptography**

Define a *cyclic code*. Define the generator and check polynomials of a cyclic code and show that they exist.

Show that Hamming's original code is a cyclic code with check polynomial $X^4 + X^2 + X + 1$. What is its generator polynomial? Does Hamming's original code contain a subcode equivalent to its dual?

4/I/4J **Coding and Cryptography**

What does it mean to transmit reliably at rate r through a binary symmetric channel (BSC) with error probability p? Assuming Shannon's second coding theorem, compute the supremum of all possible reliable transmission rates of a BSC. What happens if (i) p is very small, (ii) $p = 1/2$, or (iii) $p > 1/2$?