UNIVERSITY OF
CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday 8 June, 2006 9 to 11

PAPER 30

INFORMATION AND CODING

*Attempt **THREE** questions.*

*There are **FOUR** questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS	***SPECIAL REQUIREMENTS***
Cover sheet *Treasury Tag* *Script paper*	*None*

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 (a) Consider two discrete random variables X and Y. Define the conditional entropy $h(X|Y)$, and show that it satisfies

$$h(X|Y) \leqslant h(X),$$

giving necessary and sufficient conditions for equality. You may assume the Gibbs inequality, provided that you state it carefully.

(b) Consider two discrete random variables U and V with corresponding probability mass functions p_U and p_V. For each $\alpha \in [0,1]$, define the mixture random variable $W(\alpha)$ by its mass function

$$p_{W(\alpha)}(x) = \alpha p_U(x) + (1-\alpha) p_V(x).$$

Prove that for all α the entropy of $W(\alpha)$ satisfies:

$$h(W(\alpha)) \geqslant \alpha h(U) + (1-\alpha) h(V).$$

(c) Define $F(\lambda)$ to be the entropy of a Poisson random variable with mean $\lambda > 0$. Show that $F(\lambda)$ is a non-decreasing function of $\lambda > 0$.

2 State the Entropy Power Inequality for n-dimensional random vectors.

Let X be a real-valued random variable with a density and finite differential entropy, and let function $g : \mathbb{R} \to \mathbb{R}$ have strictly positive derivative g' everywhere. Prove that the random variable $g(X)$ has differential entropy satisfying

$$h(g(X)) = h(X) + \mathbb{E} \log_2 g'(X),$$

assuming that $\mathbb{E} \log_2 g'(X)$ is finite.

Let Y_1 and Y_2 be independent, strictly positive random variables with densities. Show that the differential entropy of the product $Y_1 Y_2$ satisfies

$$2^{2h(Y_1 Y_2)} \geqslant \alpha_1 2^{2h(Y_1)} + \alpha_2 2^{2h(Y_2)},$$

where $\log_2(\alpha_1) = 2\mathbb{E} \log_2 Y_2$ and $\log_2(\alpha_2) = 2\mathbb{E} \log_2 Y_1$.

3 (a) Prove the Hamming and Gilbert–Varshamov bounds on the size of a binary code of length N and minimum distance δ, in terms of $v_N(d)$, the volume of an N-dimensional Hamming ball of radius d.

Suppose that the minimum distance is $\lfloor \lambda N \rfloor$ for some fixed $\lambda \in (0, 1/2)$. Describe the asymptotic behaviour of both of the above bounds as $N \to \infty$.

[*You may assume that*

$$\lim_{N\to\infty} \tfrac{1}{N} \log v_N(\lfloor \lambda N \rfloor) = h(\lambda),$$

where h is the binary entropy function].

(b) State Shannon's Second Coding Theorem, giving the capacity of a general memoryless channel. Use this to calculate the capacity of a memoryless binary symmetric channel with error probability p.

(c) Fix $R \in (0, 1)$ and suppose we want to send one of a collection U_N of messages of length N, where the size $|U_N| = 2^{NR}$. The message is transmitted through a memoryless binary symmetric channel with error probability $p < 1/2$, so that we expect about pN errors. According to the asymptotic Gilbert–Varshamov bound of part (a), for which values of p can we correct pN errors, for large N? Why does this give a different answer to the Shannon capacity of part (b)?

4 Prove that the binary code of length 23 generated by the polynomial $g(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$ has minimum distance 7, and is perfect.

[*You may use the BCH theorem without proof provided it is clearly stated, and you may assume that* $X^{23} + 1 \equiv (X + 1)g(X)g^{\text{rev}}(X) \bmod 2$, *where* $g^{\text{rev}}(X) = X^{11}g(1/X)$ *is the reversal of* $g(X)$.]

END OF PAPER