UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 7 June, 2005 9 to 11

PAPER 33

INFORMATION AND CODING

*Attempt **THREE** questions.*

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

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury tag
Script paper

SPECIAL REQUIREMENTS
None

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

1 Consider two discrete probability distributions $p(x)$ and $q(x)$. Defining the relative entropy

$$D(p\|q) = \sum_x p(x) \log\left(\frac{p(x)}{q(x)}\right),$$

prove the Gibbs inequality, that is, show that $D(p\|q) \geqslant 0$, with equality iff $p(x) = q(x)$ for all x.

Using this, show that for any positive functions $f(x)$ and $g(x)$, and for any finite set A:

$$\sum_{x\in A} f(x) \log\left(\frac{f(x)}{g(x)}\right) \geqslant \left(\sum_{x\in A} f(x)\right) \log\left(\frac{\sum_{x\in A} f(x)}{\sum_{x\in A} g(x)}\right).$$

Assume that for any $0 \leqslant p, q \leqslant 1$ then

$$p \log\left(\frac{p}{q}\right) + (1-p) \log\left(\frac{1-p}{1-q}\right) \geqslant (2 \log e)(q-p)^2.$$

Show that for any probability distributions p and q:

$$D(p\|q) \geqslant \frac{\log e}{2}\left(\sum_x |p(x) - q(x)|\right)^2.$$

2 Define the conditional entropy, and show that for random variables U and V the joint entropy satisfies

$$h(U,V) = h(V|U) + h(U).$$

Given random variables $X_1, \dots X_n$, by induction or otherwise prove the chain rule

$$h(X_1, \dots X_n) = \sum_{i=1}^{n} h(X_i | X_1, \dots X_{i-1}).$$

Define the subset average over subsets of size k to be

$$h_k^{(n)} = \frac{1}{\binom{n}{k}} \sum_{S:|S|=k} \frac{h(X_S)}{k},$$

where if $S = \{s_1, \dots s_k\}$, then $h(X_S) = h(X_{s_1}, \dots X_{s_k})$. Assume that for any i, the $h(X_i|X_S) \leqslant h(X_i|X_T)$ when $T \subseteq S$, and $i \notin S$.

By considering terms of the form,

$$h(X_1, \dots X_n) - h(X_1, \dots X_{i-1}, X_{i+1}, \dots X_n)$$

show that $h_n^{(n)} \leqslant h_{n-1}^{(n)}$.

Using the fact that $h_k^{(k)} \leqslant h_{k-1}^{(k)}$, show that $h_k^{(n)} \leqslant h_{k-1}^{(n)}$, for $k = 2, \dots n$.

3 Explain what is meant by the length, size and distance of a binary code. Define a linear code by both the generator and parity check construction.

Show that the minimum distance of a linear code equals the size of the smallest linearly dependent set of rows of the parity check matrix.

Show that the Hamming code of length $2^l - 1$ is perfect, for any l.

4 (a) Prove the Plotkin bound, that for a code with size r, length N and minimum distance δ, with $2\delta > N$, the size satisfies

$$r \leqslant \frac{2\delta}{2\delta - N}.$$

(b) State the MacWilliams identity, connecting the weight enumerator polynomials of a code $\mathcal{X}$ and its dual $\mathcal{X}^{\perp}$.

Give the weight enumerator polynomial of a Hamming code of length $2^l - 1$.

END OF PAPER