UNIVERSITY OF CAMBRIDGE

M. PHIL. IN STATISTICAL SCIENCE

Friday 7 June 2002   1.30 to 4.30

QUANTUM INFORMATION THEORY

*Attempt **FOUR** questions*

*There are **five** questions in total*

The questions carry equal weight

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

1 (a) State a necessary and sufficient condition for a quantum code $\mathcal{X}$ to correct a given set $\mathcal{E}$ of errors. Under what condition does the code correct these errors non-degenerately?

(b) Prove that if a quantum code corrects E errors then it detects $2E$ errors.

(c) Describe Shor's $[[9,1]]$ quantum code and show how it can be used to correct a single phase flip error. In particular, prove that it corrects such an error degenerately.

2 How is the distance d of a quantum code defined? Prove the quantum Hamming bound. How and why does it differ from the classical Hamming bound? Use it to show that a non-degenerate $[[5,1,3]]$ code is perfect. Discuss the properties of such a code.

3 Define the Shannon entropy and von Neumann entropy, and define a classical and quantum relative entropy.

[Fano inequality] Suppose we make inference about a random variable X based on knowledge of random variable Y. If $f(Y)$ is our best guess of X, and $E = I(X \neq f(Y))$, with $p_e = P(E=1)$ show that:

$$H(X|Y) \leqslant p_e \log(|X|-1) + H(p_e),$$

where $|X|$ is the number of possible outcomes of X, and $H(p_e)$ is the entropy of E.

Hint: expand $H(E, X|Y)$ in two ways.

4 Define a quantum measurement, and give the two postulates of quantum measurement.

Show how (by communicating two classical bits) we can establish teleportation - that is, how an unknown single-qubit quantum state can be transported perfectly from A to B.

5 Assuming that the Quantum Fourier Transform can be efficiently computed, describe how the quantum phase estimation algorithm works, giving a result bounding the error probability in this algorithm.

Describe how (assuming modular exponentiation can be efficiently performed) this allows us to estimate s/r, where r is the order of $x \bmod n$.