UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2004

MEng Honours Degree in Information Systems Engineering Part IV
MSci Honours Degree in Mathematics and Computer Science Part IV
MSc in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the
Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the
Associateship of the Royal College of Science

PAPER C482=I4.44

QUANTUM COMPUTING

Tuesday 11 May 2004, 14:30
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1a (i) Show that a matrix $M \in \mathbb{C}^{n \times n}$ is unitary iff $(Mu, Mv) = (u, v)$ for all vectors $u, v \in \mathbb{C}^n$ (state clearly any properties of matrices that you may use).

(ii) Show that any eigenvalue of a unitary matrix has norm one (state clearly any properties of a unitary matrix that you may use).

(iii) Show that the eigenvectors of a unitary matrix corresponding to different eigenvalues are orthogonal.

b Explain what is meant by a *two-level* matrix. Show that any 3×3 unitary matrix can be constructed as the product of at most 3 two-level matrices.

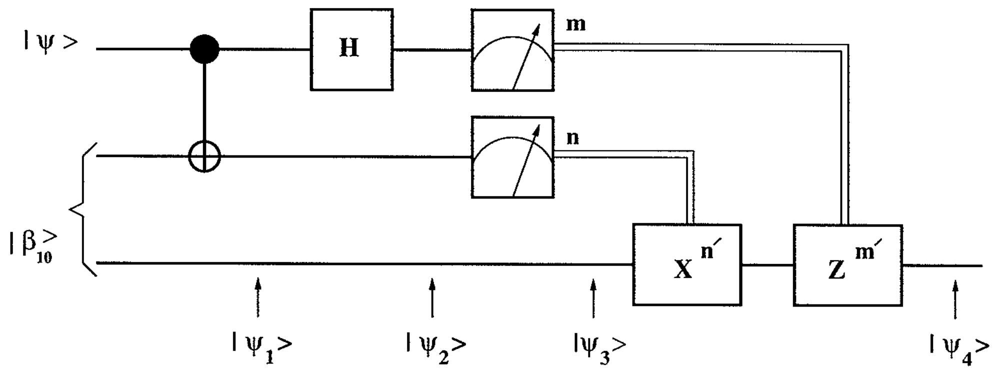
The two parts carry, respectively, 50%, 50% of the marks.

2a Define the notion of an *entangled state.* Prove that $\frac{1}{\sqrt{6}}(|100\rangle + |010\rangle + |001\rangle + |110\rangle + |011\rangle + |101\rangle)$ is an entangled state.

b Describe a two-qubit network that with input $|01\rangle$ produces the output $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

c Alice and Bob meet, generate the state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and each takes one qubit of this state. They then move apart. Now Alice wants to send the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob where α and β are unknown. They use the network in the figure below with input $|\psi\rangle \otimes |\beta_{01}\rangle$ to carry out this quantum teleportation. In this network H is the Hadamard gate, and m and n are the results of measurement by Alice of her two qubits. The Pauli matrices X and Z are given by:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$



Explain how the network is used by Alice and Bob for teleportation. Compute $|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle$ and determine m' and n' in terms of m and n such that the output $|\psi_4\rangle$ produces $|\psi\rangle$ up to a global phase.

The three parts carry, respectively, 20%, 15% 65% of the marks.

3a Define the *tensor product* $U \otimes V$ of two matrices $U \in \mathbb{C}^{n \times n}$ and $V \in \mathbb{C}^{m \times m}$.

b Assuming that U and V are both unitary, show that U and V can each be obtained from $U \otimes V$ up to a global phase constant.

c Assuming that U and V are both unitary, show by an example that U and V can only be obtained from $U \otimes V$ up to a global phase constant.

d Let N be a composite number and $y \in \{1, \cdots, N\}$ a solution of $y^2 = 1 \pmod N$ with $y \neq 1 \pmod N$ and $y \neq N - 1 \pmod N$. Show that $\gcd(y-1, N)$ and $\gcd(y+1, N)$ are non-trivial factors of N which can be computed in $O(\lceil \log N \rceil^3)$ operations.

e Assuming you are given the order finding algorithm as a black box, write down Shor's prime factorization algorithm. Run two rounds of this algorithm to factorize 35, such that, after applying the subroutine for order finding, one succeeds and one fails.

The five parts carry, respectively, 10%, 20%, 10%, 20%, 40% of the marks.

4a Find a unitary transformation U on a single qubit such that $U^2 = X$, where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

b Write down the matrix for the quantum Fourier transform on n qubits. Without giving any proofs, construct a quantum circuit to implement the Fourier transform on 3 qubits.

c A unitary matrix $U \in \mathbb{C}^{2^n \times 2^n}$ has an eigenvector u with eigenvalue $e^{2\pi i \phi}$, where ϕ is representable using three binary bits as $\phi = 0.\phi_1\phi_2\phi_3$. Design a quantum circuit to determine ϕ using a single preparation of u and black boxes to perform $\mathsf{C}(U^{2^m})$ operations for non-negative integers m, proving that your circuit can actually determine ϕ.

The three parts carry, respectively, 20%, 25%, 55% of the marks.