UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2001

BEng Honours Degree in Computing Part III
BSc Honours Degree in Mathematics and Computer Science Part III
MSci Honours Degree in Mathematics and Computer Science Part III
MSci Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing 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 C380=I4.44

QUANTUM COMPUTING

Monday 30 April 2001, 14:00
Duration: 120 minutes

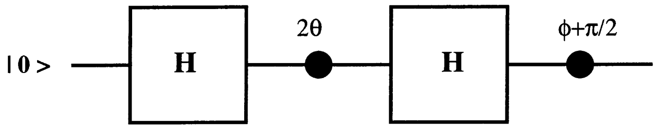
Answer THREE questions

Paper contains 4 questions
Calculators not required

1a i) Define a *unitary* transformation.

ii) Prove the No-cloning Theorem, i.e. that there is no unitary transformation which can duplicate a single qubit.

b i) Obtain the output of the network of Hadamard and phase gates in the figure below and show that by choosing the angles of phase gates appropriately, the output can be any arbitrary qubit up to an overall phase factor.



ii) Using the result of part (i) or otherwise, implement the Pauli matrix

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

in terms of the Hadamard and phase gates.

The two parts carry, respectively, 35% and 65% of the marks.

2a i) Define an *entangled state*. Prove that $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ is an entangled state.

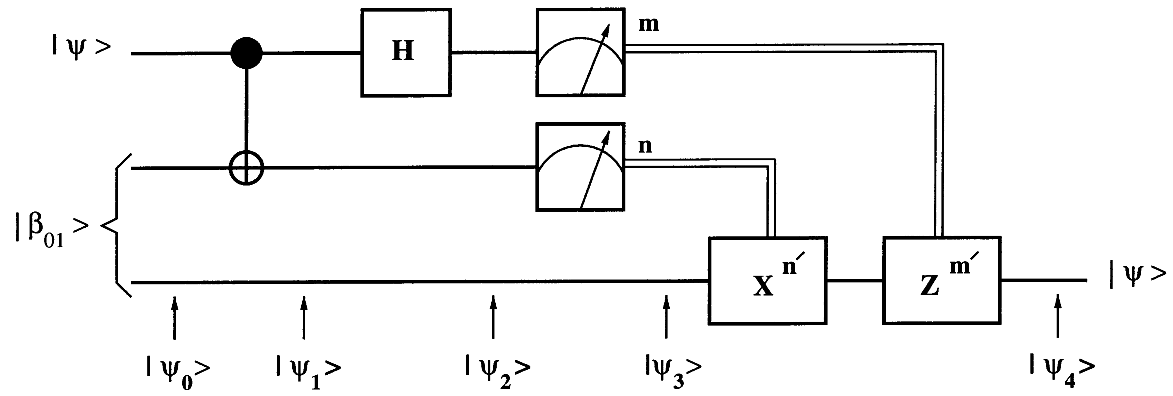
ii) Describe a two-qubit network which with input $|01\rangle$ produces the output $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

b 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. The top two qubits belong to Alice and the bottom one is Bob's. 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:

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

i) Find $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$.

ii) Determine the integers m' and n' in terms of m and n respectively so that the output of Bob's qubit is Alice's original state, i.e. $|\psi_4\rangle = |\psi\rangle$.



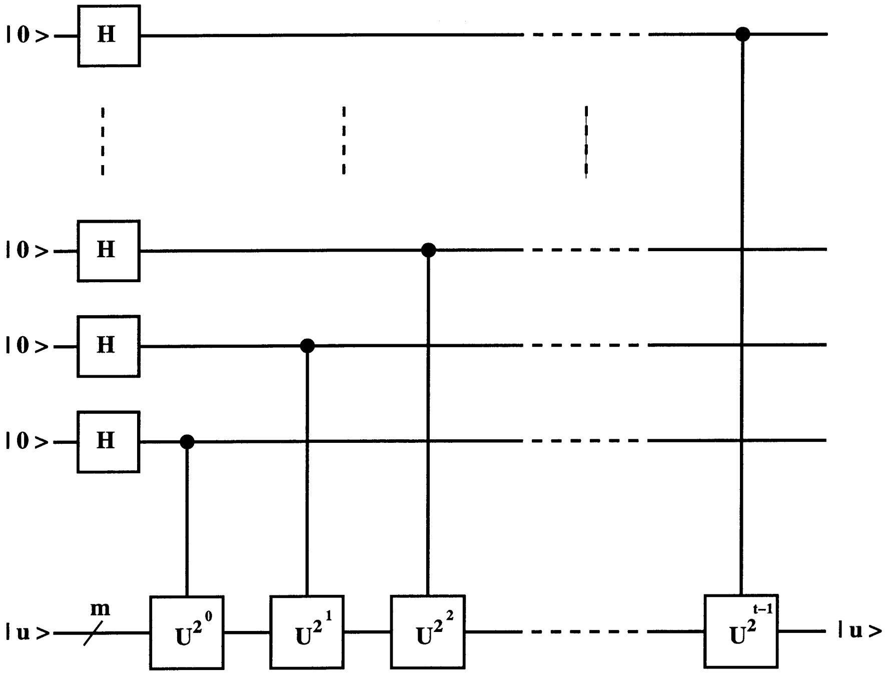
The two parts carry, respectively, 40% and 60% of the marks.

3a Define the *quantum Fourier Transform* on $\mathbb{C}^{2^n}$ and obtain its matrix representation with respect to the standard basis for $n = 2$.

b Let U be a unitary operator with eigenvalue $e^{2\pi i\phi}$ corresponding to the eigenvector $|u\rangle$. Suppose ϕ is a t-bit number, i.e. $\phi = 0.\phi_1\phi_2 \cdots \phi_t$ (written in the binary system). Assume we have a preparation of $|u\rangle$ and devices to implement the controlled U^{2^m} operations for $0 \leq m \leq t-1$.

i) Find the output of the first register (the top t qubits) in the following network.

ii) Explain carefully in technical detail how the network can be used to compute the value of ϕ.



The two parts carry, respectively, 40% and 60% of the marks.

4a i) Define the *order* of an integer x modulo N with $0 < x < N$ and $\gcd(x, N) = 1$. What is the order of 3 modulo 11?

ii) Let $0 < x < N$ and $L = \lceil \log N \rceil$. Let r be the order of x modulo N. Consider the operation U defined by:

$$U|y\rangle = |xy(\text{mod } N)\rangle,$$

for $0 \leq y \leq N - 1$ and $U|y\rangle = |y\rangle$ for $N \leq y \leq 2^L - 1$.

Show that, for $0 \leq s \leq r - 1$,

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \text{ (mod } N)\rangle,$$

is an eigenvector of U and find the corresponding eigenvalue.

b Give in detail a pseudo code for Shor's algorithm to find a non-trivial factor of a composite integer and explain its complexity.

c i) Define the *Toffoli* gate.

ii) Show that with the Toffoli gate one can construct in a reversible way any classical gate. (You should clearly state any results you may use in your proof.)

The three parts carry, respectively, 40%, 30% and 30% of the marks.