UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2003

BEng Honours Degree in Computing Part III
MSc in Computing for Industry
MEng Honours Degree in Information Systems Engineering Part IV
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
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

Tuesday 6 May 2003, 14:00
Duration: 120 minutes

Answer THREE questions

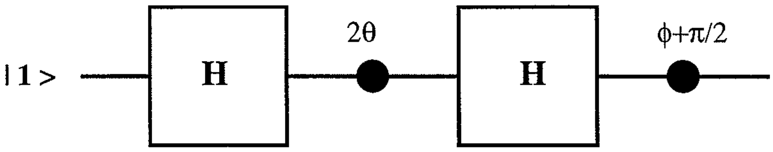
Paper contains 4 questions
Calculators not required

1a (i) Define a unitary transformation on a single qubit and write down in detail the conditions on a matrix which would represent such a transformation. Explain in detail how many real parameters are required to specify this matrix. How many of these are physically significant?

(ii) Explain the basic principle of measurement for a single qubit.

(iii) Define a quantum register with two qubits and write the general expression for such a register. What is the probability of obtaining bit 1 if the second qubit of your register is measured and what would be the resulting quantum state?

b (i) Obtain the output of the network in the figure below with $0 \leq \theta \leq \pi/2$.



(ii) Carefully locate the output of the network on the Bloch sphere.

(iii) Design a network such that with the output of the above network as its input, it outputs $|1\rangle$.

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

2a (i) Normalize the two states $\sqrt{2}|0\rangle + i|1\rangle$ and $|0\rangle - i\sqrt{2}|1\rangle$ and show that the two normalized states, which we call $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$ respectively, form a computational basis.

(ii) We measure $|0\rangle$ in the computational basis $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. What will be the probabilities of the possible outcomes and what would be the resulting states?

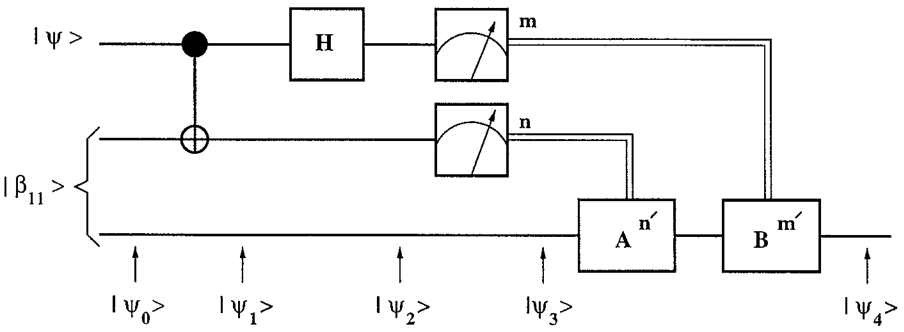
(iii) Compute the matrix representation of the NOT gate with respect to the computational basis $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$.

b (i) Define an entangled state and prove carefully that $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is entangled.

(ii) Alice and Bob meet, generate the state $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and each take 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. Explain in detail how this can be carried out using the following network, by

- describing the network fully,
- determining the intermediary states $|\psi_i\rangle$ for $i = 0, 1, 2, 3, 4$,
- determining the unitary matrices A and B and computing m' and n' in terms of m and n respectively.

(iii) Explain if this network can be reversed, justifying your answer.



The two parts carry, respectively, 30%, 70% of the marks.

3a Show the bilinearity property:
$(\alpha v + \alpha' v') \otimes (\beta w + \beta' w') = \alpha\beta v \otimes w + \alpha\beta' v \otimes w' + \alpha'\beta v' \otimes w + \alpha'\beta' v' \otimes w'$, where $\alpha, \alpha', \beta, \beta' \in \mathbb{C}$, $v, v' \in \mathbb{C}^k$, $w, w' \in \mathbb{C}^l$.

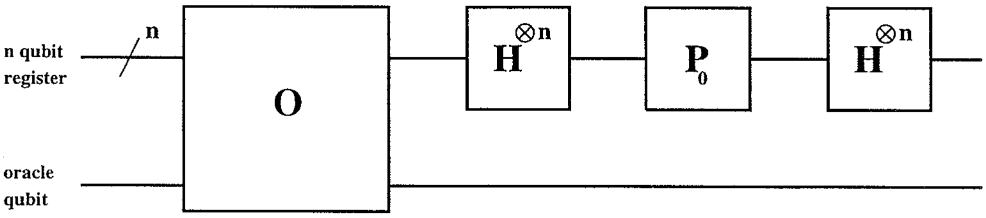
b Consider Grover's search algorithm for finding distinguished states $x \in \{0,1\}^n$ with $f(x) = 1$ where $f : \{0,1\}^n \to \{0,1\}$. Assume that the oracle O acts, for $x \in \{0,1\}^n$, as:

$$O : |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \mapsto (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Assume also that the initial state is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

with $N = 2^n$ and that the Grover operator is given by the following circuit,



where the conditional phase shift P_0 is defined as $P_0 = 2|0\rangle\langle 0| - I$ with I being the identity map.

(i) Show that O and $H^{\otimes n} P_0 H^{\otimes n}$ are both reflections in a certain real plane, which you are required to determine, and deduce the geometric action of the Grover operator.

(ii) Obtain the number of iterations required to maximize the probability of measuring one of the above distinguished states.

(ii) Assuming that n is large and there is a unique $x \in \{0,1\}^n$ with $f(x) = 1$, obtain the number of iterations needed to maximize the probability of a successful outcome of the Grover algorithm and obtain this maximum probability of success in each round of the algorithm.

The two parts carry, respectively, 25%, 75% of the marks.

4a (i) Define the quantum Fourier transform.

(ii) Obtain the two matrices representing the Fourier transform and its inverse for quantum registers with two qubits.

b (i) Define the *order* of an integer x modulo N with $0 < x < N$ and $\gcd(x, N) = 1$. Find the order of 4 modulo 21.

(ii) If r is the order of x modulo N and $L = \lceil \log N \rceil$, construct r eigenvectors and eigenvalues of the operation $U : \mathbb{C}^{2^L} \to \mathbb{C}^{2^L}$ defined by:

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

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

(iii) What linear combination of the above eigenvectors are used in the quantum phase estimation algorithm to approximate s/r for some s with $0 \leq s \leq r - 1$? Why?

c (i) Let N be a composite number and $y \in \{1, \cdots, N\}$ a solution of $y^2 = 1 \ (\text{mod } N)$ with $y \neq 1 \ (\text{mod } N)$ and $y \neq N - 1 \ (\text{mod } N)$. 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.

(ii) Explain how the order finding algorithm can be used together with (i) to obtain Shor's quantum algorithm for prime factorization. Illustrate by a successful running of Shor's algorithm to factorize 15.

The three parts carry, respectively, 20%, 35%, 45% of the marks.