UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2002

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
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=I4.32

QUANTUM COMPUTING

Thursday 2 May 2002, 14:30
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators required

1a Define the *dual* of a vector $u \in \mathbb{C}^d$, where $\mathbb{C}^d$ is the vector space of dimension d over the complex numbers $\mathbb{C}$. Define addition of dual vectors and scalar multiplication of a dual vector by a complex number. Show that the dual of a linear combination of vectors in $\mathbb{C}^d$ is a linear combination of the corresponding dual vectors. Define linear independence and the notion of a basis for the collection $(\mathbb{C}^d)^*$ of dual vectors of $\mathbb{C}^d$. Show that any basis of $\mathbb{C}^d$ induces a basis for $(\mathbb{C}^d)^*$.

b Explain the basic principle of measurement for a single qubit. Consider the three-qubit quantum register $\sum_{i,j,k\in\{0,1\}} c_{ijk}|ijk\rangle$.

(i) Compute the probability of measuring bit 0 in the first qubit and determine the state of the quantum register after this measurement.

(ii) Afterwards, i.e. having measured 0 in the first qubit, we measure the second qubit. Compute the probability of obtaining bit 1 and determine the final state of the register.

c Show that only one of the two sets

(i) $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(i|0\rangle - |1\rangle),$

(ii) $\{\frac{1}{2}(|0\rangle + \sqrt{3}|1\rangle), \frac{1}{2}(\sqrt{3}|0\rangle - |1\rangle)$

is a computational basis. Compute the outcomes and the probabilities of measuring $\alpha|0\rangle + \beta|1\rangle$ in that computational basis.

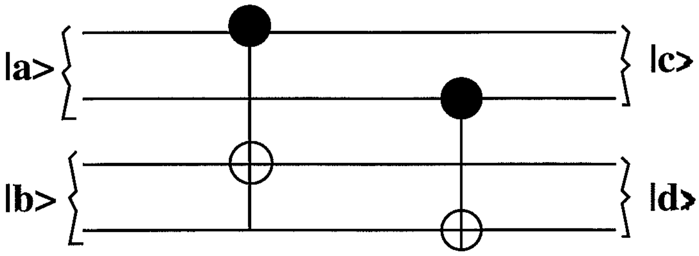
d Show that $A = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$ is unitary. Compute the action of A and of A^2 on a general qubit. What does A compute? Prove whether or not there is a classical counterpart for A.

The four parts carry, respectively, 40%, 30%, 15%, 15% of the marks.

2a (i) Define an entangled state and explain its significance and application.

(ii) What are the four Bell states?

(iii) Show that if $|a\rangle$ and $|b\rangle$ are any two Bell states of your choice then the states $|c\rangle$ and $|d\rangle$ in the output of the following circuit are both entangled.



b (i) State the No-Cloning theorem.

(ii) Prove that for any state $|a\rangle$, there exists a unitary operation U such that $U|a\rangle|0\rangle = |a\rangle|a\rangle$.

(iii) Prove that if a circuit copies two different states then these states must be orthogonal.

c Design a quantum circuit which implements the unitary matrix

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & c & 0 & 0 & 0 \\ 0 & 0 & 0 & b & d & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

using $\mathsf{C}^2(\mathsf{NOT})$ and $\mathsf{C}^2(\mathsf{A})$ gates where $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

The three parts carry, respectively, 35%, 35%, 30% of the marks.

3 Given a Boolean valued function $f : \{0,1\}^n \to \{0,1\}$, consider Grover's search algorithm for finding $x \in \{0,1\}^n$ with $f(x) = 1$. Assume that the oracle O acts, for $x \in \{0,1\}^n$, as:

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

Assume also that the initial state is

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

and that the Grover operator is given by

$$G = H^{\otimes n} P_0 H^{\otimes n} O$$

where the conditional phase shift P_0 is defined as

$$P_0 : |x\rangle \mapsto \begin{cases} |x\rangle & x = 0 \\ -|x\rangle & x > 0, \end{cases}$$

for any computational basis state $|x\rangle$ (with x in the range $0 \leq x \leq 2^n - 1$).

a Show that

$$G = (2|\psi\rangle\langle\psi| - I)O,$$

where I is the identity matrix.

b Let $R_{|\psi\rangle} = 2|\psi\rangle\langle\psi| - I$.

(i) Show that $R_{|\psi\rangle}$ reflects vectors about $|\psi\rangle$.

(ii) Show that for any vector $|\phi\rangle$, the subspace generated by the two vectors $|\psi\rangle$ and $|\phi\rangle$ is preserved by $R_{|\psi\rangle}$.

(iii) Show that for any unitary operator U we have: $UR_{|\psi\rangle}U^{-1} = R_{U|\psi\rangle}$.

c Show that the action of G is a rotation by a real angle and that this action is confined to a real plane. Describe this rotation and the real plane.

d Derive the complexity of Grover's algorithm.

e Assuming that $n \geq 2$ and that the number of x with $f(x) = 1$ is 2^{n-2}, determine how many iterates of G are required to maximise the probability of a correct outcome of the algorithm and compute this probability.

The five parts carry, respectively, 15%, 25%, 35%,15%, 10% of the marks.

4a Define the quantum Fourier transform on a register of n qubits and show that it is unitary.

b We are given positive integers x and N with $x < N$; assume $L = \lceil \log N \rceil$.

(i) Define the order r of x mod N and show that $r \leq N$.

(ii) Describe and justify in detail an algorithm to find an estimate for s/r, accurate up to 2^{2L+1} bits with probability at least $1 - \epsilon$, where s in some unknown integer in the range $0 \leq s \leq r - 1$.

c Consider Shor's quantum algorithm for factorising the integer 21. Provide two runs of the algorithm with one run failing and the other succeeding.

The three parts carry, respectively, 25%, 50%, 25% of the marks.