UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 6 June, 2014 9:00 am to 11:00 am

PAPER 61

QUANTUM COMPUTATION

Attempt no more than ***THREE*** *questions.*

There are ***FOUR*** *questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

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

1

(a) Let $f : \mathbb{Z}_N \to \mathbb{Z}_N$ be a periodic function on the integers modulo N, with period r, and which is one-to-one within each period. Suppose we are given the associated quantum oracle U_f defined by $U_f \,|\, x\rangle \,|\, y\rangle = |\, x\rangle \,|\, y + f(x) \bmod N\rangle$ with $x, y \in \mathbb{Z}_N$. Define the quantum Fourier transform QFT_N and show how r may be determined with probability $O(1/\log\log N)$ by applying at most $O(\text{poly}(\log N))$ quantum operations and classical computational steps. For the quantum operations, the application of U_f, QFT_N and measurements in the basis $\{|\, j\rangle : j \in \mathbb{Z}_N\}$ are each counted as single operations, and the only initially available quantum states are instances of the N-dimensional basis state $|\, 0\rangle$. You may use without proof any results from classical number theory but they must be stated clearly.

(b) Let B_m denote the set of all m-bit strings. For any $f : B_n \to B_1$ let U_f denote the associated quantum oracle defined by $U_f \,|\, x\rangle \,|\, y\rangle = |\, x\rangle \,|\, y \oplus f(x)\rangle$ for $x \in B_n$, $y \in B_1$ and $\oplus$ being addition mod 2. For $a = a_1 \ldots a_n$ and $x = x_1 \ldots x_n$ in B_n write $a \cdot x$ for $a_1 x_1 \oplus \ldots \oplus a_n x_n$.

(i) Suppose we are given the quantum oracle U_f for a function f promised to be of the form $f(x) = a \cdot x$ for some fixed "hidden" $a \in B_n$. Show that there is a quantum circuit that uses U_f only once, with the following property: if the input state is a string of qubits $|\, 0\rangle \ldots |\, 0\rangle$ all in state $|\, 0\rangle$ then the output state is $|\, a\rangle \,|\, A\rangle$ where $|\, a\rangle$ is an n-qubit register containing the string a and $|\, A\rangle$ is a state of any further qubits used (if needed).

(ii) In a different scenario, suppose now that access to the function $f(x) = a \cdot x$ is "concealed" by another function g in the following sense: we are given quantum oracles for two functions f and g, each on $2n$ bits defined as follows: for any $x, y, z \in B_n$ we have

$$g(x, y) = a_y \cdot x \quad \text{and} \quad f(z, x) = \begin{cases} a \cdot x & \text{if } z = a_x \\ 0 & \text{if } z \neq a_x. \end{cases}$$

Here a and a_y (for $y \in B_n$) are all fixed "hidden" strings. Thus in order to see the value $a \cdot x$ from the function f we first need to determine the corresponding string a_x contained "hidden" in the operation of the function g.

Suppose we are given quantum oracles U_f and U_g for these two functions. Show that the string a may be determined with certainty with only two queries to U_g and one query to U_f (and further quantum operations independent of f and g). [*Hint: It may be useful to consider two n-qubit registers labelled 1 and 2, initialised to the state* $\frac{1}{2^n} \sum_{x,y \in B_n} |\, x\rangle_1 \,|\, y\rangle_2$ *and reconsider the idea of (b)(i).*]

2

(i) Let $|\,\xi\rangle$ be a quantum state and introduce the operators $|\,\xi\rangle\,\langle\xi|$, $I-|\,\xi\rangle\,\langle\xi|$ and $I-2\,|\,\xi\rangle\,\langle\xi|$ (where I is the identity operation). Which of these operators are unitary? Give brief reasons for your answers.

(ii) Let $|\,\psi\rangle$ be a state vector of a quantum system and let G be a subspace of its state space. In terms of these choices, state the Amplitude Amplification Theorem.

In the following you may assume the Amplitude Amplification Theorem without proof.

(iii) Let B_n denote the set of all n-bit strings and let $f : B_2 \to B_1$ be a Boolean function with the promise that $f(x) = 1$ for a unique $x \in B_2$. Suppose we are given the corresponding quantum oracle U_f whose action is defined by $U_f\,|\,x\rangle\,|\,y\rangle = |\,x\rangle\,|\,y \oplus f(x)\rangle$ for $x \in B_2$, $y \in B_1$ (and $\oplus$ denotes addition mod 2). Show that the unique x with $f(x) = 1$ may be found with certainty using only a single query to U_f (and other quantum operations independent of f).

(iv) Suppose we are given two distinct primes p and q and the product $N = pq$ has n digits when written in binary. Consider the quantum state

$$|\,\xi\rangle = \frac{1}{\sqrt{|A|}} \sum_{k\in A} |\,k\rangle$$

where $A = \{k : 1 \leqslant k \leqslant N \text{ and } k \text{ is coprime to } N\}$, and $|A|$ denotes the size of the set A. Here all integers are written in binary as n-bit strings (adjoining leading higher order bits set to zero if needed) so $|\,\xi\rangle$ is an n-qubit state. You may assume that $|A| = (p-1)(q-1)$. Describe how the state $|\,\xi\rangle$ may be prepared with certainty in an n-qubit register, starting with any required number of qubits each initially in state $|\,0\rangle$. [*Hint: it may be useful to consider basis states $|\,k\rangle$ of n qubits extended by a single qubit prepared in a suitably chosen state.*]
Can your preparation process be implemented in poly(n) time? Give a brief reason for your answer.

3

Let U be a unitary operation on a d-dimensional state space having the following property: all eigenvalues of U are distinct and furthermore, each can be written in the form $e^{2\pi i\phi}$ with $0 < \phi < 1$ where ϕ is represented exactly in binary with n binary digits i.e. each ϕ has the form $y/2^n$ where $y = i_1 i_2 \dots i_n$ is an n-digit integer when written in binary.
Suppose we are able to implement the controlled-U operation $CU \,|\, m\rangle \,|\, \xi\rangle = |\, m\rangle \, U^m \,|\, \xi\rangle$ where $m = 0$ or 1, and we also have an eigenstate $|\, v\rangle$ of U belonging to some (initially unknown) eigenvalue $e^{2\pi i\phi}$.

(i) In terms of CU and $|\, v\rangle$ describe the Phase Estimation Algorithm and explain how it operates to provide a unitary mapping from which the eigenvalue for $|\, v\rangle$ may be read out.

(ii) Suppose we do not have an eigenstate of U. What is the output of unitary mapping of the Phase Estimation Algorithm if the eigenstate input is replaced by an arbitrary d-dimensional state $|\, \xi\rangle$?

(iii) For any given positive integer M let $U^{1/M}$ denote the principal M^{th} root of U defined to have the same eigenstates as U and corresponding eigenvalues given by $e^{2\pi i\phi/M}$ (where $0 < \phi < 1$ is as above).
If $\phi = y/2^n$ with $y = i_1 i_2 \dots i_n$ in binary, show that

$$\frac{2\pi\phi}{M} = i_1 \frac{2\pi}{2M} + i_2 \frac{2\pi}{4M} + \dots + i_n \frac{2\pi}{2^n M}.$$

Suppose now that we are given a quantum oracle for CU and for CU^{-1}, the controlled-(U^{-1}) gate. We also have an exactly universal set of quantum gates available, so in particular we are able to exactly implement any desired phase gate $P(\alpha) = \text{diag}(1 \;\; e^{i\alpha})$. Explain how we can then implement the gate $U^{1/M}$ on any d-dimensional state $|\, \xi\rangle$. [*Hint: It may be useful to consider the total effect of* $P(\alpha_1) \otimes \dots \otimes P(\alpha_n)$ *on* n *qubits in a general basis state* $|\, j_1\rangle \dots |\, j_n\rangle$.]

4

Please see below this question for a list of notations and facts that may be used without proof in this question.

(a)

(i) Explain how the action of the gate $J(\alpha)$ may be effected on a qubit in state $|\psi\rangle$ by first entangling this qubit with a second qubit and then performing a suitable 1-qubit measurement.

(ii) Consider the following quantum circuit acting on two qubits (labelled 1 and 2) prepared initially in state $|0\rangle_1 |0\rangle_2$: apply $J_1(\alpha)$, then E_{12}, then $J_2(\beta)$. Finally measure qubit 2 in the computational basis to obtain a single output bit b_2. Describe (with brief explanations) how this quantum circuit may be simulated by performing a (possibly adaptive) sequence of single qubit measurements on a suitable graph state, combined with classical deterministic processing of the measurement outcomes.

(b) In a laboratory we wish to implement a circuit C of $J(\alpha)$ and E gates containing k $J(\alpha)$ gates. The laboratory is able to perform E gates exactly but, due to difficulties with continuous variables, for each $J(\alpha)$ gate, the actual implemented gate is $J(\alpha')$ for some α' with $|\alpha' - \alpha| < \eta$.

If $|\psi_{\text{in}}\rangle$ is the input state let $|\psi_{\text{out}}\rangle = C|\psi_{\text{in}}\rangle$ denote the output state of the exact circuit, and let $|\psi'_{\text{out}}\rangle$ denote the output state of the implemented circuit. We require that $||\,|\psi_{\text{out}}\rangle - |\psi'_{\text{out}}\rangle\,|| < \epsilon$ (where $||\,|\xi\rangle\,||$ denotes the usual vector length). Determine a (non-zero) bound on η that suffices to guarantee the required condition on the output state.

Notations and facts for question 4

Quantum gates: (matrices relative to the computational basis)

$$J(\alpha) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Two qubit gate: $E = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$

(where I denotes the identity operation).

Subscripts on gate names denote the qubits to which they are applied.

Single qubit states: $|\alpha_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{-i\alpha}|1\rangle)$.

You may assume the following commutation relations:

$$\begin{aligned} J_i(\alpha)X_i^s &= e^{-is\alpha} Z_i^s J_i((-1)^s\alpha) \\ J_i(\alpha)Z_i^s &= X_i^s J_i(\alpha) \\ E_{ij}X_i^s &= X_i^s Z_j^s E_{ij} \\ E_{ij}Z_i^s &= Z_i^s E_{ij}. \end{aligned} \qquad \square$$

END OF PAPER