UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday, 10 June, 2013 9:00 am to 11:00 am

PAPER 58

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

For any positive integer M, let QFT_M denote the quantum Fourier transform mod M.

(a) Consider an M-dimensional state space with orthonormal basis $\mathcal{B} = \{|\,k\rangle : k \in \mathbb{Z}_M\}$. You may assume that QFT_M, measurements in the basis $\mathcal{B}$, and the basic arithmetic operations of addition, multiplication and division modulo M may all be performed in time $O(\mathrm{poly}(\log M))$.

Consider the function $f : \mathbb{Z}_N \to \mathbb{Z}_N$ defined by $f(x) = a^x \mod N$ where $0 < a < N$ has been chosen and is fixed. It is promised that f is periodic with period r which divides N exactly. Describe a quantum algorithm that will identify r with a constant level of probability (say 1/2) and which runs in $\mathrm{poly}(\log N)$ time. You may use without proof any results from classical number theory but they must be stated clearly.

(b) Consider an N dimensional state space with orthonormal basis $\{|\,i\rangle : i \in \mathbb{Z}_N\}$. Let S be the operation defined by $S\,|\,i\rangle = |\,i+1\rangle$ for all $i \in \mathbb{Z}_N$ (where $+$ is addition modulo N). Show that the states $\mathrm{QFT}_N\,|\,k\rangle$ for $k \in \mathbb{Z}_N$ are eigenvectors of S.
Now let $N = 4$ and represent each basis state $|\,j\rangle$ with two qubits as $|\,x\rangle\,|\,y\rangle$ where the 2-bit string xy is j written in binary. Using only the gates QFT_4, its inverse and arbitrary 1-qubit phase gates $P_\xi = \begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$ with $|\xi| = 1$, show how to implement S.

2

For any m let B_m denote the set of all m-bit strings. An oracle I_f for a Boolean function $f : B_n \to B_1$ is defined to be the n-qubit operation with action $I_f \,|\, x\rangle = (-1)^{f(x)} \,|\, x\rangle$ for all $x \in B_n$. Also write $N = 2^n$.
Consider the following oracle problem:
Problem S:
Input: an oracle I_f for a Boolean function $f : B_n \to B_1$.
Promise: f takes value 1 exactly k times. Furthermore k is known.
We say that x is "good" if $f(x) = 1$.
Problem: find a good x value.

(i) By introducing $|\,\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |\,x\rangle$ and the n-qubit operation $I_{\psi_0} = I - 2\,|\,\psi_0\rangle\,\langle\psi_0|$ (with I here being the identity operation) describe, with brief justifications, a quantum algorithm that will solve Problem S with probability at least 2/3, and which makes only $O\left(\sqrt{\frac{N}{k}}\right)$ queries to the input oracle (where you may assume that k/N is small).
Show that if $k = N/4$ then a good x value may be obtained with certainty, with just one query to the oracle.

(ii) State the Amplitude Amplification Theorem.

(iii) Suppose that for arbitrary $0 < p < 1$, and for any $0 < p' < p$, we have a quantum circuit C on n qubits with the following property:

$$\text{if} \quad |\,\psi\rangle = \textstyle\sum_{x \in B_n} a_x \,|\,x\rangle \quad \text{has} \quad \sum_{x \text{ good}} |a_x|^2 = p$$

$$\text{then} \quad C\,|\,\psi\rangle = \textstyle\sum_{x \in B_n} b_x \,|\,x\rangle \quad \text{has} \quad \sum_{x \text{ good}} |b_x|^2 = p'.$$

Show that there is a quantum algorithm that solves Problem S with *certainty* and makes $O\left(\sqrt{\frac{N}{k}}\right)$ queries to the input oracle.

3

Let $\mathbf{x} = x_0 x_1 \ldots x_{N-1}$ be an N-bit string with $N = 2K$ being even. We may think of $\mathbf{x}$ as the list of values of a function from $\mathbb{Z}_N$ to $\{0,1\}$. A quantum oracle $O_{\mathbf{x}}$ for $\mathbf{x}$ is a unitary operation on a state space of dimension $2N$ whose action is defined by $O_{\mathbf{x}} \,|\, i\rangle \,|\, y\rangle = |\, i\rangle \,|\, y \oplus x_i\rangle$, where $i \in \mathbb{Z}_N$, $y \in \{0,1\}$ and $\oplus$ denotes addition modulo 2. Consider the following two oracle problems.

Problem A:

Input: an oracle $O_{\mathbf{x}}$ for some N-bit string $\mathbf{x}$.

Promise: $\mathbf{x}$ is either a constant string, or a balanced string (the latter meaning that $\mathbf{x}$ contains exactly K 0's and K 1's).

Problem: decide if $\mathbf{x}$ is balanced.

Problem B:

Same as problem A except that the promise is omitted i.e. the input $O_{\mathbf{x}}$ may be the oracle for *any* N-bit string.

We have a universal set of quantum gates available and you may assume that any desired unitary operation that is independent of $\mathbf{x}$ may be exactly implemented.

(a) Show that Problem A can be solved with certainty by a quantum algorithm that makes only one query to the oracle $O_{\mathbf{x}}$.

(b) To develop an algorithm for problem B, we write $\hat{x}_i = (-1)^{x_i}$ and we will work on a state space of dimension N^2 with orthonormal basis states $|\, i\rangle \,|\, j\rangle$ for $i, j \in \mathbb{Z}_N$. Consider the following three computational steps:

Step 1: Make the state $|\, \psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |\, i\rangle \,|\, 0\rangle$ and then use one query to the oracle to make

$$|\, \psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \hat{x}_i \,|\, i\rangle \,|\, 0\rangle \,.$$

Step 2: Consider a transformation U whose action on states $|\, i\rangle \,|\, 0\rangle$ is given by

$$U : |\, i\rangle \,|\, 0\rangle \to \frac{1}{\sqrt{N}} \left(\sum_{k>i} |\, i\rangle \,|\, k\rangle - \sum_{k<i} |\, k\rangle \,|\, i\rangle + |\, 0\rangle \,|\, 0\rangle \right).$$

Then by linearity the action of U on $|\, \psi_1\rangle$ will be

$$|\, \psi_2\rangle = U \,|\, \psi_1\rangle = \left(\frac{1}{N} \sum_{i=0}^{N-1} \hat{x}_i \right) |\, 0\rangle \,|\, 0\rangle + \sum_{i<j} \frac{(\hat{x}_i - \hat{x}_j)}{N} \,|\, i\rangle \,|\, j\rangle \,.$$

[You may assume without proof that this formula is correct.]

Step 3: Measure $|\, \psi_2\rangle$ to obtain an outcome (k, l) with $k, l \in \mathbb{Z}_N$.

(i) Show that there exists a *unitary* transformation $\tilde{U}$ on the whole state space whose action on the states $|\,i\rangle\,|\,0\rangle$ coincides with the action of U as given in step 2.

(ii) Suppose that the promise of Problem A is imposed. If we see $(0,0)$, respectively $(i,j) \neq (0,0)$, as the measurement outcome in step 3, what can we deduce about the string $\mathbf{x}$?

(iii) Now returning to general input strings $\mathbf{x}$ and considering the possible measurement outcomes (k,l), show that Problem B may be solved with certainty with at most $K = N/2$ queries to the oracle in every case (by using a suitable extension of the three steps above, or otherwise).

4

(a) In this question you may assume the following two lemmas.

Lemma A: Let A and B be Hermitian matrices with $||A|| \leqslant \eta$ and $||B|| \leqslant \eta$ for some real $\eta \leqslant 1$ (where $||A||$ denotes the spectral norm of A). Then

$$e^{-iA}e^{-iB} = e^{-i(A+B)} + O(\eta^2).$$

Lemma B: Let $U_1, \ldots, U_K$ and $V_1, \ldots, V_K$ be unitary matrices with $||U_i - V_i|| \leqslant \eta$ for all $i = 1, \ldots, K$. Then $||U_1 \ldots U_K - V_1 \ldots V_K|| \leqslant K\eta$.

Consider the following Hamiltonian on n qubits labelled as $0, 1, \ldots, n-1$:

$$H = \sum_{i=1}^{n} X_{i-1}\, Z_i$$

and let $U = e^{iH}$. Here the operators X and Z are the standard 1-qubit Pauli operators and X_j denotes the n-qubit operation of X acting on the j^{th} qubit and the identity operation on all other qubits (and similarly for Z_j).

(i) Find $||X_0\, Z_1||$.

(ii) Let $\epsilon > 0$ be given. Explain how an operation $\tilde{U}$ with $||U - \tilde{U}|| < \epsilon$ may be implemented by a poly(n) sized circuit of 2-qubit gates, and identify the degree of the polynomial. You may assume that $1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 = O(n^3)$.

(b)

(i) For any Hamiltonian H and unitary operation W show that

$$W^\dagger e^{iH} W = e^{iW^\dagger H W}$$

where $\dagger$ denotes the adjoint.

(ii) Consider the Boolean function $f(x_1 \ldots x_n) = x_1 \oplus \ldots \oplus x_n$ where $x_1 \ldots x_n$ is an n-bit string and $\oplus$ denotes addition mod 2. Describe a circuit of 2-qubit gates on $n+1$ qubits that implements the transformation $|\, x_1 \ldots x_n \rangle\, |\, 0 \rangle \to |\, x_1 \ldots x_n \rangle\, |\, x_1 \oplus \ldots \oplus x_n \rangle$.

(iii) By considering a relationship between f and the n-qubit Hamiltonian $Z \otimes \ldots \otimes Z$, or otherwise, show that $V = \exp(i\, Z \otimes \ldots \otimes Z\, t)$, for any fixed $t > 0$, may be implemented on n qubit lines (with possible use of further ancillary lines) by a circuit of size $O(n)$ of 1- and 2-qubit gates.

END OF PAPER