UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 27 May, 2016 1:30 pm to 3:30 pm

PAPER 324

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

(i) Define the *order* of α mod N for integers α and N with $\alpha < N$ coprime. Compute the order of 7 mod 15. Explain briefly how knowledge of the order of α mod N can be used to provide a factor of N, stating the conditions on α and its order that must be satisfied. Illustrate the procedure in the case of $\alpha = 7$ and $N = 15$.

(ii) Outline the steps involved in Shor's quantum algorithm for finding a factor of an integer N. Any significant theorems that you invoke to justify the algorithm should be clearly stated. In particular you may quote without proof the following result from the theory of continued fractions:
Theorem CF: For any given rational number $0 < a/b < 1$ with a and b coprime integers having at most n digits each, let p/q be any rational number (with p and q coprime) satisfying $\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{1}{2q^2}$. Then there are only $O(n)$ such fractions p/q and they can all be classically computed from a/b in $O(n^3)$ time. Furthermore their denominators are all less than or equal to b.

(iii) Consider applying Shor's algorithm to factorise $N = 15$, with $\alpha < N$ coprime having been chosen to be 7. Determine the probability that a single run of Shor's algorithm for this particular choice of α and N will output a factor of 15 (different from 1 and 15 itself).

2

(a) Let $\mathcal{H}$ be a finite dimensional state space and let $\mathcal{G} \subseteq \mathcal{H}$ be a linear subspace. Let $|\psi\rangle$ be any state in $\mathcal{H}$.
Define the operator I_ψ of reflection in the hyperplane orthogonal to $|\psi\rangle$, and the operator $I_\mathcal{G}$, of reflection in the subspace $\mathcal{G}^\perp$ orthogonal to $\mathcal{G}$. In terms of these, state and prove the Amplitude Amplification Theorem.

Now write $[N] = \{0, 1, 2, \ldots, N-1\}$ and let $\mathcal{H}$ have dimension N with orthonormal basis $\{|x\rangle : x \in [N]\}$.

(b) Suppose we are given a quantum oracle U_g for a function $g : [N] \to \{0,1\}$. If $\mathcal{G} = \mathrm{span}\{|x\rangle : g(x) = 1\}$, describe how $I_\mathcal{G}$ may be implemented using U_g and other quantum operations that are independent of g. (For any g the quantum oracle U_g acts on $\mathcal{H}$ with an extra qubit adjoined, and it is defined by $U_g |x\rangle |k\rangle = |x\rangle |k \oplus g(x)\rangle$ for all $x \in [N]$ and $k \in \{0,1\}$; and here $\oplus$ denotes addition mod 2.)

(c) In this question you may assume that for any classically computable function $g : [N] \to \{0,1\}$, we can implement the corresponding quantum oracle U_g (defined as in (b) above), and for any state $|\psi\rangle \in \mathcal{H}$, we can implement I_ψ.

Suppose we are given the quantum oracle U_f for a function $f : [N] \to [N]$ i.e. U_f acts on $\mathcal{H} \otimes \mathcal{H}$ by $U_f |x\rangle |y\rangle = |x\rangle |y + f(x)\rangle$ for all $x, y \in [N]$ and here $+$ denotes addition mod N.
It is promised that f is a one to one function. We wish to find an $x \in [N]$ with the property that $f(x)$ is a perfect square (for usual integer multiplication i.e. $f(x)$ is 1 or 4 or 9 etc.) We should succeed with probability at least 0.9 (independently of the size of N).
Show that the quantum query complexity of this task (for queries to U_f) grows as $O(N^{1/4})$.

3

Let I, X, Z denote the identity operator and standard Pauli operators on a single qubit. Let $\mathcal{P}_1$ denote the set comprising I, X, Z, XZ and their multiples by ± 1 and $\pm i$. Let $\mathcal{P}_n = \{A_1 \otimes A_2 \otimes \ldots \otimes A_n : A_j \in \mathcal{P}_1 \text{ for } j = 1, \ldots, n\}$. An n-qubit unitary operation U is called a *Clifford operation* if it preserves $\mathcal{P}_n$ under conjugation i.e. for any $A_1 \otimes A_2 \otimes \ldots \otimes A_n \in \mathcal{P}_n$ there is an $A'_1 \otimes A'_2 \otimes \ldots \otimes A'_n \in \mathcal{P}_n$ such that

$$U^\dagger \left(A_1 \otimes A_2 \otimes \ldots \otimes A_n\right) U = A'_1 \otimes A'_2 \otimes \ldots \otimes A'_n. \tag{1}$$

You may assume that the Hadamard gate H, the phase gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, and the controlled-$Z$ gate CZ are all Clifford operations (when acting on any of the n qubit lines).

(i) Suppose that U in eq. (1) is H or S or CZ, acting on any specified qubit line(s). Show that if we are given the list $A_1, A_2, \ldots A_n$ then the list of operators $A'_1, A'_2, \ldots, A'_n$ may be determined by a classical computation of only poly(n) time.

(ii) Let $Z_1 = Z \otimes I \otimes \ldots \otimes I$ denote Z acting on the first of n qubit lines. If $|\psi\rangle$ is any n-qubit state, show that

$$\langle \psi | Z_1 | \psi \rangle = p_0 - p_1 \tag{2}$$

where p_0 and p_1 are the probabilities of obtaining outcomes 0 and 1 respectively, from a computational basis measurement on the first qubit of $|\psi\rangle$.

(iii) Now let $C = U_N \ldots U_2 U_1$ with $N = O(\text{poly}(n))$ be any poly-sized quantum circuit of H, S and CZ gates on n qubit lines. Consider a computational process with C being applied to any product input state $|a_1\rangle |a_2\rangle \ldots |a_n\rangle$ and with the output being obtained by a computational basis measurement on the first qubit line. Let p_0 and p_1 be the probabilities of obtaining outputs 0 and 1 respectively. Show that if we are given the list $U_1, \ldots, U_N$ of gates of C (including the lines on which they act), and the identities of the 1-qubit states $|a_1\rangle, \ldots, |a_n\rangle$, then we can classically compute p_0 and p_1 in classical poly(n) time i.e. any such quantum process offers no computational time speed up over classical computing (up to polynomial overheads).

(iv) Show that it is possible for circuits C of the type in (iii) to generate n-qubit states $|\psi\rangle = C |0\rangle |0\rangle \ldots |0\rangle$, from the starting state $|0\rangle |0\rangle \ldots |0\rangle$, such that each qubit of $|\psi\rangle$ is entangled with the subsystem comprising all the remaining qubits.

4

(i) Define the spectral norm $||A||$ of an operator A.
Let $\{U_i\}$ and $\{V_i\}$ be sets of m unitary operators with $||U_i - V_i|| < \epsilon$ for $i = 1, \ldots, m$. Show that $||U_m \ldots U_1 - V_m \ldots V_1|| < m\epsilon$. [You may assume that the spectral norm satisfies the triangle inequality.]

(ii) Let $H = \sum_{k=1}^{M} H_k$ be a 2-local Hamiltonian on n qubits with $M = O(n^2)$, and suppose that the operators H_k satisfy $||H_k|| < 1$ for $k = 1, \ldots, M$.
Show how $U = e^{-iH}$ may be approximated to within ϵ in spectral norm, by a circuit of 2-qubit gates. The circuit size should scale as $O(1/\epsilon)$ and polynomially in n. You should identify the degree of the polynomial growth in n. [You may use the Lie-Trotter product formula without proof, but in that case, it should be clearly stated.]

END OF PAPER