UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday, 6 June, 2017 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

Throughout this question, for any integer N let $\mathbb{Z}_N$ denote the set of integers modulo N. Let $\mathcal{H}_N$ denote an N dimensional state space with standard orthonormal basis $\mathcal{B} = \{|\,0\rangle, \ldots, |\,N-1\rangle\}$. You may assume that measurements relative to the basis $\mathcal{B}$ and the quantum Fourier transform mod N may both be implemented in poly($\log N$) time. You may also assume that the number of integers less than N that are coprime to N grows as $O(N/\log\log N)$ and that $x \in \mathbb{Z}_N$ has a multiplicative inverse mod N iff x and N are coprime.

(a) Let $f : \mathbb{Z}_N \to \mathbb{Z}_N$ be a periodic function which is one-to-one within each period and which can be computed by a poly($\log N$) sized circuit. Explain how the period r of f can be determined in poly($\log N$) time by a quantum computation which succeeds with probability $O(1/\log\log N)$, and after which we also learn if the computation has been successful or not.

(b) For any prime p consider the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} \subset \mathbb{Z}_p$ of nonzero integers modulo p, with the operation of multiplication mod p. A *generator* for $\mathbb{Z}_p^*$ is an element g whose powers generate all of $\mathbb{Z}_p^*$ i.e. for all $x \in \mathbb{Z}_p^*$ there is $y \in \mathbb{Z}_{p-1}$ with $x = g^y \mod p$. y is called the *discrete logarithm* of x (to base g). You may assume that $\mathbb{Z}_p^*$ always has a generator g and that it satisfies $g^{p-1} \equiv 1 \mod p$.

Suppose we are given a generator g and element $x \in \mathbb{Z}_p$, and we wish to compute its discrete logarithm y.

(i) Consider the function $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ given by

$$f(a, b) = g^a x^{-b} \mod p.$$

For each fixed $c \in \mathbb{Z}_p^*$, show that there is a corresponding fixed $k \in \mathbb{Z}_{p-1}$ such that

$$f(a, b) = c \quad \text{iff} \quad a = by + k \mod p-1.$$

(ii) Suppose we have constructed the state

$$|\,\phi\rangle = \frac{1}{(p-1)} \sum_{a,b \in \mathbb{Z}_{p-1}} |\,a\rangle\,|\,b\rangle\,|\,f(a,b)\rangle$$

(in $\mathcal{H}_{p-1} \otimes \mathcal{H}_{p-1} \otimes \mathcal{H}_p$) and we measure the third register obtaining a result c_0. Find the post-measurement state of the first two registers.

(iii) If we then apply the quantum Fourier transform mod $(p-1)$ to each of these two registers and measure both registers, which output pairs $(c_1, c_2) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ can be obtained with non-zero probability? Can y be determined from any such pair? Give a reason for your answer.

2

(a) Let $\mathcal{B}_n$ denote the set of all n-bit strings and write $N = 2^n$. Let $f : \mathcal{B}_n \to \mathcal{B}_1$ be a function taking value 1 exactly k times, with $f(x) = 1$ iff $x \in G = \{x_1, \ldots, x_k\}$. The Grover operator is defined by $Q = -H_n I_0 H_n I_G$ where $H_n = H \otimes \ldots \otimes H$ is the Hadamard operation on each of n qubits, and for all $x \in \mathcal{B}_n$, I_0 and I_G are defined by

$$I_0 \,|\, x\rangle = \begin{cases} -\,|\, x\rangle & \text{if } x = 0\ldots0 \\ \;\;|\, x\rangle & \text{if } x \neq 0\ldots0 \end{cases} \qquad I_G \,|\, x\rangle = \begin{cases} -\,|\, x\rangle & \text{if } x \in G \\ \;\;|\, x\rangle & \text{if } x \notin G. \end{cases}$$

Write $|\,\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathcal{B}_n} |\, x\rangle$. Derive a geometrical interpretation of the action of Q in a suitable part of the space of n qubits, which should be clearly defined. Using this interpretation, show that if I_G is given as a black box then an x in G may be obtained with high probability (better than a half say) with $O(\sqrt{N/k})$ uses of I_G, if N is large and k is small compared to N.

(b) Let $g : \mathcal{B}_n \to \mathcal{B}_n$ be a 2-to-1 function i.e. for every y in the range of g there are precisely two strings $x \in \mathcal{B}_n$ with $g(x) = y$. A *collision* is a pair of strings $x_1, x_2 \in \mathcal{B}_n$ with $g(x_1) = g(x_2)$. The standard quantum oracle U_g for g is the unitary operation on $2n$ qubits defined by

$$U_g \,|\, x\rangle \,|\, y\rangle = |\, x\rangle \,|\, y \oplus g(x)\rangle \qquad x, y \in \mathcal{B}_n$$

where $\oplus$ denotes bitwise addition of n-bit strings.

Suppose that we are given U_g as a black box operation. Using the result of (a), or otherwise, show that a collision may be found with high probability (better than a half say) with $O(N^{1/3})$ uses of U_g.
[Hint: start by partitioning the domain of g into sets A and B of sizes $N^{1/3}$ and $(N - N^{1/3})$ and listing all the values of $g(x)$ for $x \in A$. We might find a collision there, but if we're not so lucky, what should we do next with B?]

3

(a) Let ϕ be a real number satisfying $\phi = c/2^n$ for some known integer n and unknown integer c with $0 \leqslant c < 2^n$. Let U be a unitary operator, and let $|\,\psi\rangle$ be a quantum state such that $U\,|\,\psi\rangle = e^{2\pi i\phi}\,|\,\psi\rangle$.

Describe a quantum algorithm which, given access to a controlled-U operation and the ability to produce $|\,\psi\rangle$, outputs ϕ exactly. Give an explanation of the correctness of your algorithm and include a quantum circuit for it. (You may treat the inverse quantum Fourier transform (QFT^{-1}) as a black box in your circuit, i.e. you need not give a circuit for QFT^{-1}).

(b) Let A be an n-qubit Hermitian operator with all eigenvalues λ_i distinct and each having the form $\lambda_i = c_i/2^n$ for an integer $0 \leqslant c_i < 2^n$. Suppose further that we are able to implement the unitary $U = e^{2\pi i A}$ and its controlled version controlled-U.

We are given an n-qubit state $|\,b\rangle$ (as a quantum physical state, with its actual identity possibly unknown) and we wish to produce the state $|\,\psi\rangle$ given by the vector $A\,|\,b\rangle$ normalised, with some non-zero probability. We have available a universal set of gates and in particular we are able to implement controlled rotations of the form

$$|\,c\rangle\,|\,0\rangle \longrightarrow |\,c\rangle\;(\cos\theta_c\,|\,0\rangle + \sin\theta_c\,|\,1\rangle)$$

where $0 \leqslant c < 2^n$ is an integer and $\sin\theta_c = c/2^n$. Here the first and second registers are an n-qubit and one-qubit register respectively.

(i) Let $|\,u_j\rangle$ be a normalised eigenvector of A belonging to λ_j, and let $|\,b\rangle = \sum \beta_j\,|\,u_j\rangle$. Show how we can construct the state

$$\sum \beta_j\sqrt{1-\lambda_j^2}\,|\,u_j\rangle\,|\,c_j\rangle\,|\,0\rangle + \beta_j\lambda_j\,|\,u_j\rangle\,|\,c_j\rangle\,|\,1\rangle$$

from $|\,b\rangle$. Here the first two registers are each n-qubit registers and the third is a one-qubit register.

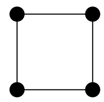
(ii) Hence (or otherwise) show how the state $|\,\psi\rangle$ may be obtained with probability of success exceeding the square of the smallest eigenvalue of A.

4

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

(a) (i) State how the operation $J(\alpha)$ may be applied to a qubit in any state $|\psi\rangle$ by using only the operation E and a suitable single qubit measurement (and any ancillary qubits in suitable fixed states as needed). You need not prove the validity of your claimed process.

(ii) Consider the graph state $|\psi_{2\times 2}\rangle$ corresponding to the graph

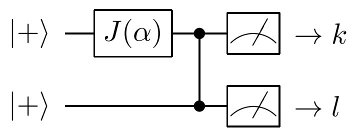


Using the formula given below for the action of E (or otherwise) show that if one of the qubits is measured in the computational basis with result r, the remaining qubits will be left in the state $(Z^r \otimes I \otimes Z^r)\,|\psi_3\rangle$, where $|\psi_3\rangle$ is the graph state corresponding to the graph

(iii) Next, the first qubit of the state $(Z^r \otimes I \otimes Z^r)\,|\psi_3\rangle$ is measured in the basis $\{|\alpha_+\rangle, |\alpha_-\rangle\}$, and result s is obtained. (Here $s = 0$ respectively 1 corresponds to the first, respectively second, vector in the measurement basis). Show that the remaining qubits (now labelled 2 and 3) are left in the state

$$E_{23}\, X_2^{(r+s)}\, J(\alpha)_2\; Z_3^r\; |+\rangle_2\, |+\rangle_3 .$$

(iv) Using your previous answers, explain how you could simulate the results of the circuit



using single-qubit measurements on $|\psi_{2\times 2}\rangle$ and classical processing of the results. (In the above diagram the final boxes on the two lines denote standard basis measurements with outcomes k and l respectively.)

(b) In measurement-based computing, what does it mean for a measurement pattern to have *logical depth 1*? Let $\mathcal{C}$ be any quantum circuit on a single qubit, comprising only $H = J(0)$ and $J(\pi/2)$ gates before a final standard basis measurement. The initial state of the qubit is $|+\rangle$. Show that $\mathcal{C}$ may be simulated by a measurement pattern with logical depth one. *[Hint: it may be useful to note that $J(-\pi/2) = XJ(\pi/2)$.]*

NOTATIONS AND FACTS FOR QUESTION 4

Quantum gates:

X and Z denote the standard Pauli gates.

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

E denotes the two qubit controlled-Z gate and it maps $|a\rangle |b\rangle$ to $(-1)^{ab} |a\rangle |b\rangle$ for $a, b \in \{0, 1\}$.

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

Single qubit states:

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

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

You may assume the following commutation relations:

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

END OF PAPER