UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday, 31 May, 2012 1:30 pm to 3:30 pm

PAPER 67

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

Let $\mathbb{Z}_N$ denote the set of integers modulo N. The quantum Fourier transform mod N has matrix elements (relative to a chosen orthonormal basis $\mathcal{B} = \{|\,0\rangle\,, \ldots, |\,N-1\rangle\}$ of an N-dimensional state space):

$$[\mathrm{QFT}_N]_{ab} = \frac{1}{\sqrt{N}} w^{ab} \quad \text{where } a, b \in \mathbb{Z}_N \text{ and } w = e^{2\pi i/N}.$$

(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. Assuming that QFT_N and measurements relative to the basis $\mathcal{B}$ can be implemented in poly($\log N$) time, explain how the period r of f can be determined in poly($\log N$) time by a quantum computation that succeeds with probability $O(1/\log\log N)$, and we also learn if the computation has been successful or not. [You may also assume that the number of integers less than N that are coprime to N grows as $O(N/\log\log N)$.]

(b) A qutrit is a quantum system that has a 3-dimensional state space with a chosen orthonormal basis denoted $\{|\,0\rangle\,, |\,1\rangle\,, |\,2\rangle\}$. Consider the function $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ defined by $f(x_1, x_2) = a_1 x_1 + a_2 x_2 \bmod 3$, where $a_1, a_2 \in \mathbb{Z}_3$ are constants. Consider also the associated operation on three qutrits defined by

$$U_f\,|\,x_1\rangle\,|\,x_2\rangle\,|\,y\rangle = |\,x_1\rangle\,|\,x_2\rangle\,|\,y + f(x_1, x_2) \bmod 3\rangle$$

for all $x_1, x_2, y \in \mathbb{Z}_3$.
Let S denote the single qutrit operation defined by $S\,|\,x\rangle = |\,x + 1 \bmod 3\rangle$ for $x \in \mathbb{Z}_3$.
Show that $|\,\xi\rangle = \mathrm{QFT}_3\,|\,2\rangle$ is an eigenstate of S.
Suppose now that we are given an oracle for U_f but a_1 and a_2 are unknown. By suitable use of $|\,\xi\rangle$ (or otherwise) show that the pair (a_1, a_2) may be determined by a single application of U_f together with further operations that are independent of f.

2

This question is about lower bounds on quantum query complexity in the model where the quantum algorithm is given access to bits of an unknown input x via an oracle.

(a) Sketch a proof that, if there exists a quantum algorithm which computes a boolean function $f(x)$ with certainty on all inputs x, using T queries to x, then f is represented by a multilinear polynomial of degree at most $2T$.

Consider the "majority" boolean function $\text{MAJ} : \{0,1\}^3 \to \{0,1\}$, which is defined by

$$\text{MAJ}(x) = \begin{cases} 0 & \text{if } |x| \leqslant 1 \\ 1 & \text{otherwise,} \end{cases}$$

where $|x|$ is the Hamming weight of $x \in \{0,1\}^3$, i.e. the number of 1s in x.

(b) Write down the multilinear polynomial that represents MAJ, and hence show that any quantum algorithm computing $\text{MAJ}(x)$ with certainty on all inputs x must make at least two queries to x.

(c) Describe a quantum algorithm which computes $\text{MAJ}(x)$ exactly for all inputs x and makes two queries to x. You may assume the existence of a quantum algorithm which computes the function $\text{PARITY}(y) = y_1 \oplus y_2$ exactly for any $y \in \{0,1\}^2$, using one query to y.

Now consider the function $\text{MAJ}_n : \{0,1\}^{3n} \to \{0,1\}$, which is defined as follows. Split the input $(x_1, \dots, x_{3n})$ into n contiguous blocks $b_1, \dots, b_n$ of 3 bits each, and set $\text{MAJ}_n(x) = 1$ if and only if $\text{MAJ}(b_i) = 1$ for all $i \in \{1, \dots, n\}$. For example,

$$\text{MAJ}_2(x_1, \dots, x_6) = \text{MAJ}(x_1, x_2, x_3) \wedge \text{MAJ}(x_4, x_5, x_6).$$

(d) Show that any quantum algorithm computing $\text{MAJ}_n(x)$ with certainty on all inputs x must make at least $3n/2$ queries to x.

(e) If f is a boolean function which has block sensitivity b, any quantum algorithm which computes $f(x)$ with bounded error must make at least $\Omega(\sqrt{b})$ queries to x. Assuming this result, or otherwise, show that any quantum algorithm computing $\text{MAJ}_n(x)$ with bounded error must make at least $\Omega(\sqrt{n})$ queries to x.

3

Please see the page following this question for a list of notations used and statements of two lemmas that may be assumed without proof.

(a) Consider the following quantum circuit C on two qubits prepared initially in the state $|+\rangle_1 |+\rangle_2$: apply $J_1(\alpha)$, then $J_2(\beta)$, then E_{12}, then $J_2(\gamma)$. Finally measure the two qubits in the computational basis to obtain an output pair of bits (b_1, 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, followed by classical deterministic processing of the measurement outcomes.

(b) The logical depth of a (possibly adaptive) measurement pattern on a graph state is the number of layers of simultaneous measurements that is needed to perform all the measurements.
Let D be any circuit comprising only $H = J(0)$ and CX gates (on nearest neighbour qubits) with input state $|+\rangle_1 |+\rangle_2 \ldots |+\rangle_n$. Show that D may be simulated by a measurement pattern of logical depth one (on a suitable graph state). [*Hint: it may be useful to note that* $CX_{ij} = H_j E_{ij} H_j$.]

(c) Let $R(\alpha)$ denote the gate $R(\alpha) = J(\alpha)J(0)$. The commutation relations in lemma 2 below easily imply the following facts:
Fact 1: $R(\alpha)$ commutes with X.
Fact 2: CX has the following Pauli propagation relations:

$$CX_{ij}\, X_i = X_i X_j\, CX_{ij} \qquad CX_{ij}\, X_j = X_j\, CX_{ij}.$$

[You are not required to derive these facts!] Using these facts (or otherwise) show that any circuit comprising only CX and $R(\alpha)$ gates (using any desired set of α values) may be simulated by performing a measurement pattern of logical depth two (on a suitable graph state).

NOTATIONS AND LEMMAS FOR QUESTION 3

Single qubit states:

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

Single qubit measurements:
$M_i(\alpha)$ denotes measurement of the i^{th} qubit in the orthonormal basis $\{|\,\alpha_+\rangle\,, |\,\alpha_-\rangle\}$. The measurement outcome corresponding to $|\,\alpha_+\rangle$ (resp. $|\,\alpha_-\rangle$) is taken to be 0 (resp. 1).

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 gates:

$$E = |\,0\rangle\,\langle 0\,| \otimes I + |\,1\rangle\,\langle 1\,| \otimes Z$$
$$CX = |\,0\rangle\,\langle 0\,| \otimes I + |\,1\rangle\,\langle 1\,| \otimes X$$

(where I denotes the identity operation). Subscripts on gate names will denote the qubits to which they are applied. The 2-qubit gates E_{ij} and CX_{ij} will always be assumed to be applied to nearest-neighbour qubits i.e. $j = i \pm 1$.

You may assume the following two lemmas:

Lemma 1 ("J-lemma"). Consider two qubits initialised in state $|\,\psi\rangle_1\,|\,+\rangle_2$ (where $|\,\psi\rangle$ is an arbitrary qubit state). If we apply E_{12} followed by the measurement $M_1(\alpha)$, then the second qubit is left in state $X^s J(\alpha)\,|\,\psi\rangle$ where $s \in \{0, 1\}$ is the measurement outcome. □

Lemma 2 ("Pauli propagation relations"). The following relations hold for $s \in \{0, 1\}$:

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

4

This question is about quantum phase estimation. Throughout the question, let ϕ be a real number satisfying $\phi = x/2^m$ for some known integer m and unknown integer x such that $0 \leqslant x \leqslant 2^m - 1$.

(a) 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. Include a proof of correctness of your algorithm.

(b) Write down a quantum circuit for your algorithm. 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}.

Let U_ϕ be the unitary operator on one qubit defined by

$$\begin{aligned} U_\phi|0\rangle &= \frac{1}{2}\left((1+e^{2\pi i\phi})|0\rangle + (1-e^{2\pi i\phi})|1\rangle\right), \\ U_\phi|1\rangle &= \frac{1}{2}\left((1-e^{2\pi i\phi})|0\rangle + (1+e^{2\pi i\phi})|1\rangle\right). \end{aligned}$$

(c) Calculate the eigenvalues and eigenvectors of U_ϕ. Hence show that, given access to a controlled-U_ϕ operation as a black box, ϕ can be determined exactly with $O(2^m)$ uses of U_ϕ.

Let $U_\phi^{(n)}$ be the unitary operator on n qubits defined by

$$U_\phi^{(n)}|x\rangle = \left(\frac{1+e^{2\pi i\phi}}{2}\right)^n \sum_{y\in\{0,1\}^n} \left(\frac{1-e^{2\pi i\phi}}{1+e^{2\pi i\phi}}\right)^{|x\oplus y|} |y\rangle,$$

where $|x \oplus y|$ is the Hamming weight of $x \oplus y$, i.e. the number of bits in which x and y differ.

(d) Suppose that n is a power of 2 and $\phi < 1/n$. Show that, given access to a controlled-$U_\phi^{(n)}$ operation as a black box, ϕ can be determined exactly with $O(2^m/n)$ uses of $U_\phi^{(n)}$.

END OF PAPER