UNIVERSITY OF CAMBRIDGE

MAT3, MAMA

MATHEMATICAL TRIPOS Part III

Thursday, 30 May, 2019 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
Rough 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) (i) Give a statement of the *hidden subgroup problem* for a finite group G.

(ii) Let G be a finite abelian group and $\mathcal{H}$ a state space with orthonormal basis $\{|g\rangle : g \in G\}$ labelled by the elements of G. Define the shift operator $U(h)$ for $h \in G$, acting on $\mathcal{H}$. Describe how a common eigenbasis for all the shift operators may be constructed and identify their corresponding eigenvalues. You may use results from group representation theory without proof but they should be clearly stated.

(iii) In the course of the standard quantum algorithm for the abelian hidden subgroup problem for abelian group G with hidden subgroup K of size $|K|$, we obtain a coset state of the form

$$|g_0 + K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 + k\rangle$$

where $g_0 \in G$ has been chosen uniformly at random. Show how the constructions in (ii) can be used to provide a measurement, which when applied to $|g_0 + K\rangle$, has an output distribution that is independent of g_0, and depends only on the hidden subgroup K.

(b) For any suitable set Y let $f : \mathbb{Z}_N \to Y$ be a surjective function which is periodic with period $r \in \mathbb{Z}_N$ and with $f(0), f(1), \ldots, f(r-1)$ all being distinct. Let $\mathcal{H}_Y$ be a state space with orthonormal basis labelled by the elements of Y, and let U_l for $l \in \mathbb{Z}_N$ be the operation on $\mathcal{H}_Y$ defined by $U_l\,|f(x)\rangle = |f(x+l)\rangle$ for all $x \in \mathbb{Z}_N$.
Consider the state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle\,|f(x)\rangle$ and let $|\xi\rangle$ be the result of applying the quantum Fourier transform over $\mathbb{Z}_N$ to the first register of $|\psi\rangle$. Show that $|\xi\rangle$ may be expressed as

$$|\xi\rangle = \frac{1}{\sqrt{|M|}} \sum_{x \in M} |x\rangle\,|e_x\rangle$$

where the $|e_x\rangle$'s are normalised common eigenvectors of all the operators U_l for $l \in \mathbb{Z}_N$, and $M \subseteq \mathbb{Z}_N$ of size $|M|$, is a subset of $\mathbb{Z}_N$ which should be determined. Hence determine how the result of measuring the second register of $|\xi\rangle$ in the common eigenbasis of the U_l's depends on the period r.

2

(a) Let $\mathcal{H}$ be a finite dimensional state space and let $\mathcal{G} \subseteq \mathcal{H}$ be a linear subspace. In terms of these, state and prove the Amplitude Amplification theorem.

(b) Let $\mathcal{H}_K$ denote a state space of dimension K with orthonormal basis $\{|k\rangle : k \in \mathbb{Z}_K\}$. For any $h : \mathbb{Z}_N \to \mathbb{Z}_M$ let U_h denote the unitary operation on $\mathcal{H}_N \otimes \mathcal{H}_M$ defined by $U_h |x\rangle |y\rangle = |x\rangle |y + h(x) \bmod M\rangle$ for all $x \in \mathbb{Z}_N$ and $y \in \mathbb{Z}_M$.

(i) Let S on $\mathcal{H}_K$ be defined by $S|x\rangle = |-x \bmod K\rangle$ for all $x \in \mathbb{Z}_K$. Show that S is unitary.

(ii) For h as above let r be the function $r(x) = -h(x) \bmod M$. Suppose we are given a quantum oracle for the operation U_h. Show that U_h and U_r are inverse operations, and that U_r may be implemented with a single use of U_h and other gates that are independent of h.

Suppose now that we are given a quantum oracle U_f for $f : \mathbb{Z}_N \to \mathbb{Z}_N$ and it is promised that f is a one-to-one function. We wish to find $x \in \mathbb{Z}_N$ satisfying $f(x)^4 \leqslant N$. Here for $0 \leqslant f(x) < N$, $f(x)^4$ is computed in $\mathbb{Z}$ i.e. not reduced $\bmod N$. Call such x's good, and all other x's bad. We should succeed in finding a good x with probability at least 0.9 asymptotically for all large N.

(iii) Let I_g be the operator defined by $I_g|x\rangle = -|x\rangle$ if x is good and $I_g|x\rangle = |x\rangle$ if x is bad. Show that I_g can be implemented with two uses of U_f and other gates that are independent of f. [*Hint: it may be useful to incorporate the result of (ii) for a suitable choice of h there.*]

(iv) Hence or otherwise show that the quantum query complexity (for queries to U_f) of the task of finding a good x is at most $O(N^{3/8})$.

3

(a) Let X and Z denote the standard 1-qubit Pauli operators, and let X_j denote the n-qubit operation of X acting on the j^{th} qubit with the identity operation on all other qubits (and similarly for Z_j).

(i) Define the spectral norm $||A||$ of any operator A. Find $||X_1 Z_2||$.

(ii) State the Lie-Trotter product formula.

(iii) 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 $U = e^{-iH}$. For any given $\epsilon > 0$, 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 should state clearly any properties of the spectral norm that you use (which may be used without proof).

(b) Let B_n denote the set of all n-bit strings. Consider the n-qubit operation A defined by

$$A\,|x\rangle = (-1)^{f(x)}\,|x\rangle \qquad \text{for all } x \in B_n$$

where $f : B_n \to B_1$ is a function which is quantum-computable in the following sense: there is a circuit C of 1-qubit and 2-qubit gates that implements the operation $U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$ for $x \in B_n$ and $y \in B_1$ (and $\oplus$ denotes addition mod 2).

(i) A is both unitary and Hermitian. Given an n-qubit register, introduce an extra qubit labelled as qubit $n+1$ and write $\tilde{A} = A \otimes I_{n+1}$ where I_{n+1} is the identity operation on qubit $n+1$. Show how $\tilde{A}$ acting as a unitary operation on $|x\rangle\,|0\rangle_{n+1}$ for any $x \in B_n$, may be implemented using only the gates of C, their inverses and a suitable Pauli gate.

(ii) Now view A as a Hermitian Hamiltonian. Using (i) or otherwise, show how $U = e^{iA}$ may be implemented on an n-qubit register by a circuit of 1-qubit and 2-qubit gates.

4

(a) Consider the linear system of equations $Ax = b$ with $x, b \in \mathbb{C}^N$ and A Hermitian. Write $n = \log N$. Suppose all eigenvalues of A lie in the interval $[0, 1]$ and that each eigenvalue has the form $x/2^n$ for an integer $0 \leqslant x < 2^n$, so eigenvalues can be exactly represented in n bits.

(i) State the further conditions on A and b that are needed for the Harrow-Hassidim-Lloyd (HHL) quantum algorithm to apply to the linear system and run in time $O(\text{poly}(n))$, to produce with success probability at least $O(1/\text{poly}(n))$, an n-qubit quantum state $|\xi\rangle$ corresponding to the solution vector x normalised.

(ii) Describe the steps of the HHL algorithm. You may assume that any use of phase estimation or Hamiltonian simulation can be executed exactly and their actions may be quoted without proof. You should also state clearly the actions of any operations independent of A and b that are needed.

(b) The HHL algorithm uses a multi-qubit controlled operation W of the following general form. For any n-bit string x let $0 \leqslant \theta_x \leqslant \pi/2$ be a value that can be classically efficiently computed given x. Then W, operating on an n-qubit control register and a 1-qubit target register, gives the following transformation for any n-bit string x:

$$|x\rangle\,|0\rangle \longrightarrow |x\rangle\,(\cos\theta_x\,|0\rangle + \sin\theta_x\,|1\rangle)\,.$$

Here the two registers comprise n qubits and one qubit respectively. Show how W can be implemented as a circuit of 1-qubit and 2-qubit gates of size $\text{poly}(n)$. You may ignore any issues of precision, assuming that all needed quantities can be adequately represented in $O(n)$ bits.

END OF PAPER