UNIVERSITY OF CAMBRIDGE

MAMA/324, NST3AS/324, MAAS/324

MAT3

MATHEMATICAL TRIPOS Part III

Thursday 6 June 2024 9:00 am to 11:00 am

PAPER 324

QUANTUM COMPUTATION

Before you begin please read these instructions carefully

Candidates have TWO HOURS to complete the written examination.

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

Let $G = \langle g \rangle$ be a cyclic group of order N, generated by the element g. For any $x \in G$, the unique $\eta \in \mathbb{Z}_{N-1}$ satisfying $x = g^\eta$ is called the *discrete logarithm* of x to the base g. Let $\mathcal{H}_N$ be an N-dimensional state space with standard orthonormal basis $\mathcal{B} = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. For each $\alpha \in \mathbb{Z}_N$, let $U(\alpha)$ denote the associated shift operator acting on $\mathcal{H}_N$, acting as $|\beta\rangle \mapsto |\beta + \alpha\rangle$ for all $\beta \in \mathbb{Z}_N$ (where $+$ denotes addition in $\mathbb{Z}_N$). Denote by F_N the quantum Fourier transform over $\mathbb{Z}_N$, and let $\omega := e^{2\pi i/N}$ be a primitive N^{th} root of unity. You may use the identity $\sum_{\alpha \in \mathbb{Z}_N} \omega^\alpha = 0$ without proof wherever required.

(a) Define the *hidden subgroup problem* for G.

(b) Explain what is meant by a *shift invariant basis* for $\mathcal{H}_N$. Show that the states $|\xi_\alpha\rangle := \frac{1}{\sqrt{N}} \sum_{\beta \in \mathbb{Z}_N} \omega^{-\alpha\beta} |\beta\rangle$ for $\alpha \in \mathbb{Z}_N$ form such a basis.

(c) Let $\mathcal{H}$ be a state space with orthonormal basis $\{|k\rangle : k \in G\}$ labeled by the elements of G. For $\alpha \in \mathbb{Z}_N$ define the state $|\chi_\alpha\rangle \in \mathcal{H}$ by

$$|\chi_\alpha\rangle := \frac{1}{\sqrt{N}} \sum_{\beta \in \mathbb{Z}_N} \omega^{\alpha\beta} |g^\beta\rangle \, .$$

For $x, y \in G$ and $\alpha \in \mathbb{Z}_N$, define the "division operator" D_x over $\mathcal{H}_N \otimes \mathcal{H}$ by

$$D_x |\alpha\rangle |y\rangle = |\alpha\rangle |y x^{-\alpha}\rangle,$$

where $x^{-\alpha}$ is the inverse of x^α in G.

(i) Show that D_x is unitary.

(ii) Show that $|\alpha\rangle|\chi_\beta\rangle$ is an eigenvector of D_x and compute its eigenvalue.

(iii) Compute the output state on applying the operator $(F_N^\dagger \otimes I) D_x (F_N \otimes I)$ to the state $|\alpha\rangle|\chi_\beta\rangle$.

(iv) Given an element $x \in G$ as input, explain how you can use the result of part (iii) above to find the discrete logarithm of x to the base g. You may assume the ability to implement D_x and F_N efficiently, and to prepare the state $|\chi_\beta\rangle$ for any β of your choice.

2

(a) Let $\mathcal{H}$ be a finite dimensional Hilbert space, and let $\mathcal{G} \subseteq \mathcal{H}$ be a linear subspace. Let $|\psi\rangle \in \mathcal{H}$ be any normalised state. Define the necessary reflection operators, and in terms of these state the Amplitude Amplification Theorem as it applies to $\mathcal{G}$ and $|\psi\rangle$.

(b) Suppose we are given an m-qubit unitary U that performs the map

$$U|0^m\rangle = \sqrt{p}|\psi_1\rangle|1\rangle + \sqrt{1-p}|\psi_0\rangle|0\rangle,$$

where $|\psi_0\rangle$ and $|\psi_1\rangle$ are arbitrary normalised $(m-1)$-qubit states and $p \in (0,1)$ is unknown. Let $\mathcal{S}$ be the 2-dimensional subspace spanned by $|\psi_0\rangle|0\rangle$ and $|\psi_1\rangle|1\rangle$.

(i) Compute the action of the operator $I_{m-1} \otimes Z$ (where I_{m-1} is the $(m-1)$-qubit identity operator and Z is the single qubit Pauli Z gate) in $\mathcal{S}$ and show that it reflects in the hyperplane orthogonal to $|\psi_1\rangle|1\rangle$.

(ii) Let $R_0 = I_m - 2|0^m\rangle\langle 0^m|$. Show that in $\mathcal{S}$, the unitary $UR_0U^\dagger$ is a reflection in the hyperplane orthogonal to $U|0^m\rangle$. [*Hint: It may help to extend $U|0^m\rangle$ to an orthonormal basis for $\mathcal{S}$.*]

(iii) Show that in $\mathcal{S}$, the unitary $UR_0U^\dagger \cdot (I_{m-1} \otimes Z)$ is a rotation. What is the relation between the angle of rotation and p?

(iv) Suppose the value of p is known and it is greater than $1/4$. Explain how the state $|\psi_1\rangle$ can be prepared exactly using the rotation in part (iii) above. You may use ancillary qubits, and assume the ability to prepare arbitrary single qubit states.

3

Denote the standard single-qubit Pauli operators by I, X, Y, Z. For any single-qubit operator P let P_j denote the n-qubit operator that acts as P on the j^{th} qubit and as the identity on all other qubits. Let J_X and J_Z be the n-qubit operators defined as

$$J_X = \sum_{i=1}^{n} X_i, \quad J_Z = \frac{1}{2} \sum_{\substack{i,j=1 \\ i \neq j}}^{n} Z_i Z_j.$$

(a) Define the *spectral norm* $\|O\|$ of an operator O. Show that $\|J_X\| \leqslant n$.

(b) Show that quantum evolution for time $t > 0$ under the Hamiltonian J_X can be implemented exactly using a circuit of only $3n$ elementary gates. You may assume access to a two-qubit universal gate set consisting of the Hadamard operator H, CNOT, and phase gates of the form $\text{diag}(1, e^{i\alpha})$ for all $\alpha \in [0, 2\pi)$.

(c) Now let $J = J_X + J_Z$. Is J a k-local Hamiltonian for k independent of n? Explain how to use the second order product formula

$$e^{-iA/2} e^{-iB} e^{-iA/2} = e^{-i(A+B)} + E,$$

where $\max\{\|A\|, \|B\|\} \leqslant \Lambda$ and E is an operator with $\|E\| = O(\Lambda^3)$, to simulate quantum evolution under the Hamiltonian J for time $t > 0$ and precision ϵ in spectral norm. You may use without proof that if $\|U_i - V_i\| \leqslant \epsilon$ for $i = 1, \ldots, n$, then $\|U_n \ldots U_1 - V_n \ldots V_1\| \leqslant n\epsilon$. How does the size of the simulating circuit scale with n, t and ϵ?

4

Suppose we are given an oracle that implements an unknown unitary U on n qubits, but we do not have an oracle for $U^\dagger$ or for controlled-U. We are also given an eigenvector $|v_0\rangle$ of U corresponding to the eigenvalue 1, and another arbitrary n-qubit state $|b\rangle$ as quantum physical states (with their actual identities or classical descriptions being unknown). We have access to a universal set of quantum gates, and in particular for $j = 1, 2, \ldots$ we can implement phase gates of the form

$$P(j) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^j} \end{pmatrix}.$$

(a) Using ideas from the Harrow-Hassidim-Lloyd (HHL) algorithm, explain how to prepare the state $U^\dagger|b\rangle$ using only poly(n) queries to U. You may assume that all the eigenvalues of U can be written as $\lambda_j = e^{2\pi i\phi_j}$ with $\phi_j = c_j/2^m$ for some m-bit integers $0 \leqslant c_j < 2^m$, where $m = O(\log n)$.

(b) State the conditions required on the vector b for the HHL algorithm to be applicable to the linear system defined by $Ux = b$, and to run in time $O(\text{poly}(n))$.

(c) The HHL algorithm uses a single qubit rotation controlled on m qubits, of the following form. For any m-bit string x, suppose that $0 \leqslant \theta_x \leqslant \pi/2$ is a parameter that can be efficiently computed classically from x. Then the operator W acts on $m + 1$ qubits, implementing the map

$$W|x\rangle|0\rangle = |x\rangle \left(\cos\theta_x|0\rangle + \sin\theta_x|1\rangle\right)$$

for every $x \in \{0,1\}^m$. Assuming that all the required quantities can be represented in $O(m)$ bits and ignoring any precision issues, show how to implement W as a circuit of size poly(m) using 1-qubit and 2-qubit gates. You may use ancillary qubits if necessary.

END OF PAPER