UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Wednesday, 2 June, 2021 12:00 pm to 2:00 pm

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.

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 Let G be a finite (generally non-abelian) group of size $|G|$ and let $\mathcal{H}$ be a state space with orthonormal basis $\{|\, g\rangle\}_{g\in G}$ labelled by the elements of G.

(a) Give a statement of the hidden subgroup problem for G.

Let $f : \mathbb{Z}_K \to \mathbb{Z}$ be a periodic function that is one-to-one within each period. Explain how the problem of determining the period of f can be formulated as a hidden subgroup problem for a suitable group, identifying explicitly all the ingredients in the formulation.

(b) Let $\chi^{(1)}, \ldots, \chi^{(L)}$ be a complete set of unitary irreps for G with $\chi^{(\alpha)}$ having dimension d_α for $\alpha = 1, 2, \ldots, L$. Let $\chi^{(\alpha)}(g)$ have matrix elements $M_{\alpha,ij}(g)$ for $1 \leqslant i, j \leqslant d_\alpha$ and $g \in G$, and introduce the vectors (for each α, i, j)

$$|\, \alpha_{ij}\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \overline{M}_{\alpha,ij}(g)\, |\, g\rangle$$

(where the overline denotes complex conjugation).

(i) State how the unitary quantum Fourier transform operator on $\mathcal{H}$ is constructed in terms of the above ingredients. Any results from group representation theory may be quoted without proof but they should be clearly stated.

(ii) For each $g_0 \in G$ introduce the linear operator $U(g_0)$ on $\mathcal{H}$ defined by $U(g_0)\,|\, g\rangle = |\, g_0 g\rangle$ for all $g \in G$. For a subgroup H of G and any $g \in G$, introduce the coset state $|\, gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h\in H} |\, gh\rangle$ (where $|H|$ is the size of H).
For each irrep label α, show that the action of $U(g_0)$ preserves the d_α^2-dimensional subspace $\mathcal{H}_\alpha$ spanned by $|\, \alpha_{ij}\rangle$ for $1 \leqslant i, j \leqslant d_\alpha$, and identify its action on that subspace (in terms of g_0 and the irrep matrices).
Hence or otherwise show that the incomplete measurement that distinguishes only the $\mathcal{H}_\alpha$ subspaces, when applied to $|\, gH\rangle$, has output probability distribution Π independent of the choice of g i.e. Π depends only on the choice of subgroup H.

(iii) Is the output distribution Π above necessarily different for different subgroups H? Give a reason for your answer.

2 (a) Let U be a unitary operation on n qubits that we are able to implement in poly(n) time, and suppose also that we are able to implement $U^{(2^k)}$ in poly(n,k) time. We are also given an eigenstate $|\,\xi_0\rangle$ of U with known eigenvalue 1.

With all the above, suppose we are now given a further eigenstate $|\,\xi\rangle$ of U, having eigenvalue λ that is unknown, but promised to be of the form $\lambda = e^{2\pi i\phi}$ with $\phi = c/2^m$ for integers c and m with $0 \leqslant c \leqslant 2^m - 1$. Show (with the aid of suitable circuit diagrams if desired) how c may be determined in a time that grows polynomially in n and m. Also give a brief justification that your proposed method has the required poly(n,m) time bound.

(b) Let A be an n-qubit Hermitian operator with all eigenvalues λ_i being distinct and $0 < \lambda_i < 1$ for all i. Suppose that we are able to implement the $(n+1)$-qubit operations $C\text{-}U_\pm$ which are the controlled operations corresponding to the unitary operators $U_\pm = e^{\pm 2\pi i A}$ respectively.

We are given a single instance of an n-qubit state $|\,b\rangle$ (as a quantum physical state) and we wish to produce the state $|\,\psi\rangle$ given by the vector $e^A\,|\,b\rangle$ normalised. For implementing quantum operations we have available a universal set of quantum gates. Show how the state $|\,\psi\rangle$ may be obtained with a non-zero probability of success P_S and give a positive lower bound for P_S that is independent of $|\,b\rangle$.
[You may ignore issues of precision, and assume that all needed numerical quantities can be adequately represented in $O(n)$ bits.]

3 (a)(i) State the Amplitude Amplification Theorem as it applies to a subspace $\mathcal{G}$ of a state space $\mathcal{H}$ and state $|\,\psi\rangle \in \mathcal{H}$.

(ii) Suppose we have a quantum factoring algorithm that operates as follows. For any n-bit integer N, there is a classical poly(n) time algorithm that given N, outputs a description of a poly(n)-sized quantum circuit C_N on n qubits. Then C_N is run on $|\,0\rangle^{\otimes n}$ and all lines are measured. The resulting output x (viewed as an n-bit integer) has the property that if N is composite then x is a (non-trivial) factor of N with probability equalling $\sin^2(\pi/10)$.

Given the above, show how we may construct a poly(n) time quantum algorithm that outputs a factor of N with certainty if N is composite. You should include a justification that your proposed algorithm runs in poly(n) time. [You may assume that the n-qubit operation $I - 2\,|\,00\ldots0\rangle\,\langle 00\ldots0\,|$ (with I being the identity operation) is implementable in poly(n) time.]

(b) Consider the Harrow-Hassidim-Lloyd (HHL) algorithm as applied to the linear system $A\underline{x} = \underline{b}$, for $\underline{x} \in \mathbb{C}^N$ and A being a Hermitian $N \times N$ matrix. You may assume that A and $\underline{b}$ satisfy all the properties required for the HHL algorithm to apply.

Define the *condition number* κ of A. Suppose now that all eigenvalues of A are in the interval $[0,1]$. By briefly outlining the steps of the HHL algorithm or otherwise, explain why the requirement that κ be $O(\text{poly}(\log N))$ is needed if the algorithm is to run in $O(\text{poly}(\log N))$ time, to produce its output state corresponding to the vector $A^{-1}\underline{b}$ normalised, with any constant level of probability (independent of N).

4 Consider a quantum computational process denoted summarily as $\mathcal{C}(|\,\psi_0\rangle\,, C, K)$, defined as follows. We have a specified quantum poly-time circuit C on n qubits labelled $1, \ldots, n$, with input being the product state $|\,\psi_0\rangle = |\,\alpha_1\rangle \ldots |\,\alpha_n\rangle$, and output given by a computational basis measurement on a subset of K specified lines, labelled $i_1, \ldots, i_K$.

(i) Define what it means for the output of the process to be *classically strongly efficiently simulatable.*

(ii) Define the notion of a *Clifford operation.* Suppose now that the circuit C in $\mathcal{C}(|\,\psi_0\rangle\,, C, K)$ is made of gates from the set $\{H, CX, S\}$ (where H is the Hadamard gate, CX the controlled X gate and S is the $\pi/2$ phase gate), and $K = 1$ with $i_1 = 1$. Show that the output is classically strongly efficiently simulatable.
[You may assume that H, CX and S are all Clifford operations.]

(iii) Introduce now the extra (non-Clifford) gate $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$. You may assume that $\{H, CX, S, T\}$ is a universal set of gates for quantum computation. You may also assume that the action of T on any qubit line j may be implemented by an adaptive Clifford process (called the T-gadget) of the following form: we introduce an extra ancillary qubit (labelled a) in state $|\,A\rangle = \frac{1}{\sqrt{2}}\left(|\,0\rangle + e^{i\pi/4}\,|\,1\rangle\right)$, apply CX_{ja}, measure line a to obtain a result $m = 0$ or 1, and finally apply S^m to line j. The ancillary qubit line is not used again.

Given all the above, consider computational processes of the form $\mathcal{C}(|\,\psi_0\rangle\,, C, K)$ for poly(n)-sized Clifford circuits C of gates from $\{H, CX, S\}$ (and having no intermediate measurements) and arbitrary product state inputs $|\,\psi_0\rangle$, and now with $K \geqslant 1$ (instead of just $K = 1$ as in (ii) above).

Show that if any such $\mathcal{C}(|\,\psi_0\rangle\,, C, K)$ is classically strongly efficiently simulatable for any $1 \leqslant K \leqslant n$ then we would have P = BQP i.e. if D is any decision problem that can be solved in quantum poly-time with bounded error, then we would have that D can be solved in classical deterministic poly-time.

END OF PAPER